

Documento Final

Yeison Ferreira, Edu Nievas, David Hidalgo
David Vallès, Maite Torres
2nC SMX

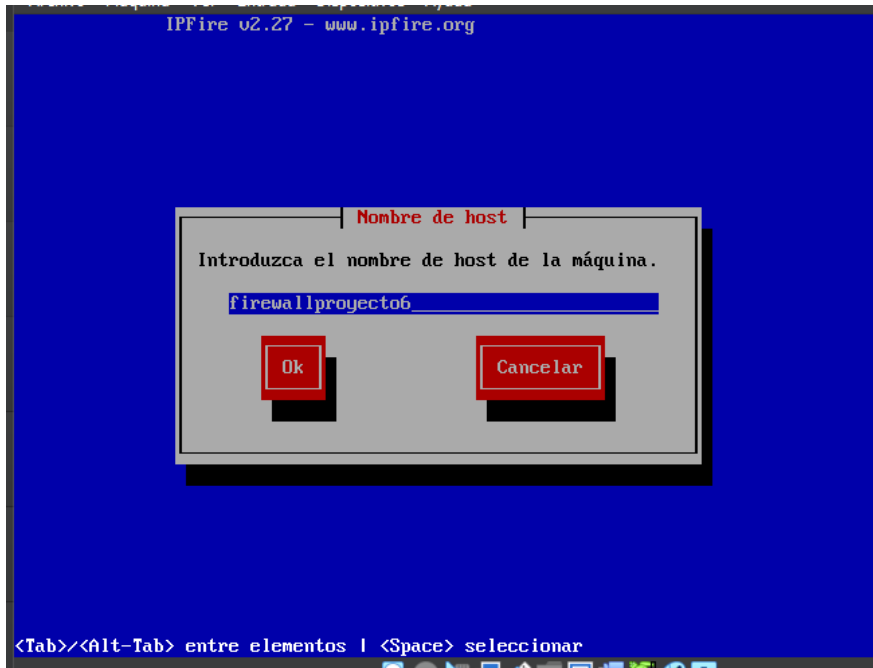
Índice

Fase 1 – Control de xarxa	3
1- Configuració d'un firewall de la xarxa	3
2- Configuració d'un proxy que limiti el contingut al que poden accedir els equips de la xarxa	14
Fase 2 – Migració Wordpress on-premise	20
1- Selecció del sistema operatiu i serveis que habilitareu per a poder migrar l'actual wordpress que teniu allotjat al núvol cap a una infraestructura on premise (hosting).	20
2- Guia de configuració de les diferents instal·lacions i serveis per a entregar-ho al client.	33
3- Configuració del servei dins d'una infraestructura segura.	39
Fase 3 – Gestió de documents (6h)	43
1- Instal·lació d'un sistema d'emmagatzemament en xarxa.	43
2- Selecció dels serveis que habilitareu per a que els usuaris de l'empresa puguin compartir recursos centralitzats i en xarxa de dades.	56
3- Guia de configuració dels diferents serveis per entregar-ho al client.	61
Fase 4 – Configuració de backups i hardening (3h)	66
1- Configuració dels backups de les dades en un disc en xarxa.	66
2- Estableix criteris de complexitat de contrasenyes i contra atacs de força bruta per l'accés als equips.	84
Conclusión	89

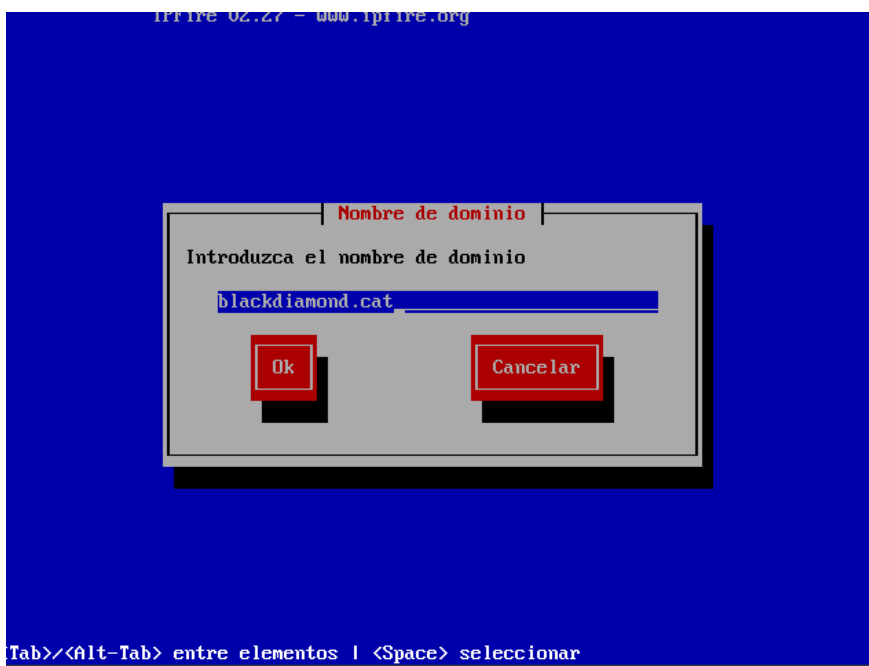
Fase 1 – Control de xarxa

1- Configuració d'un firewall de la xarxa

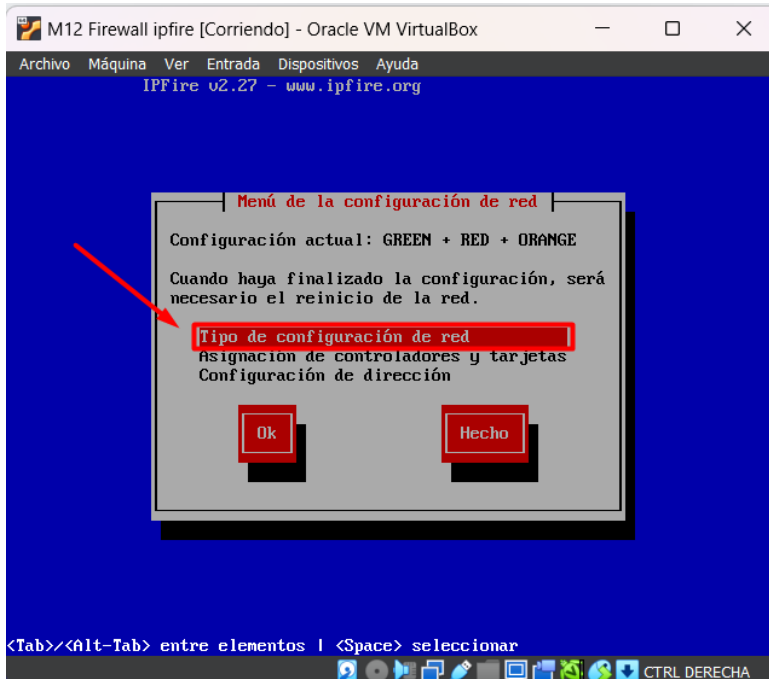
Lo primero que se pedirá al empezar la configuración del firewall (IPFire), será el hostname de la máquina, en el que se pondrá: "firewallproyecto6".



Seguidamente, se tendrá que introducir el nombre del dominio de la red, esta será "blackdiamond.cat".



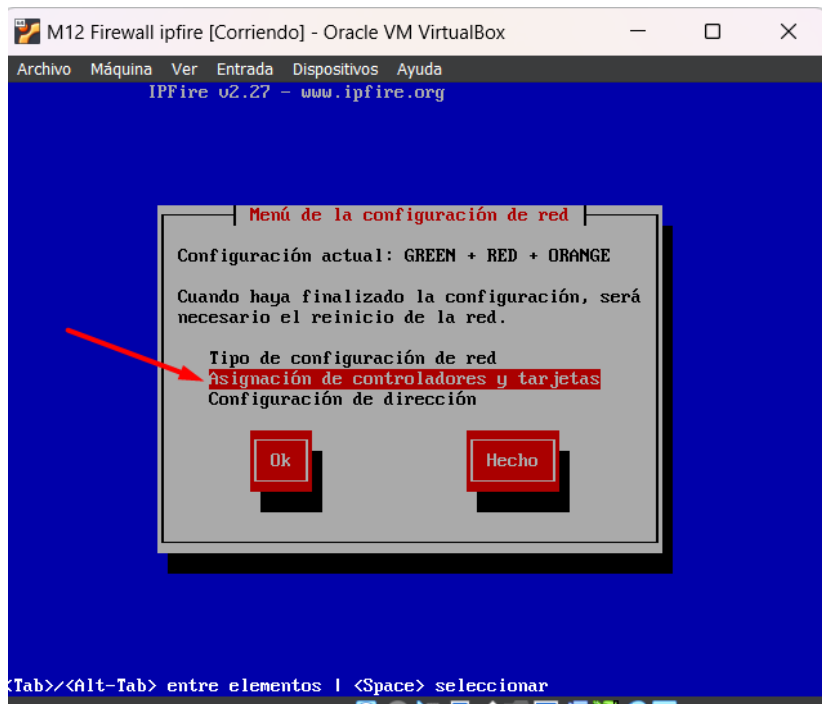
Una vez se acceda a la configuración de red, se accederá a "Tipo de configuración de la red".



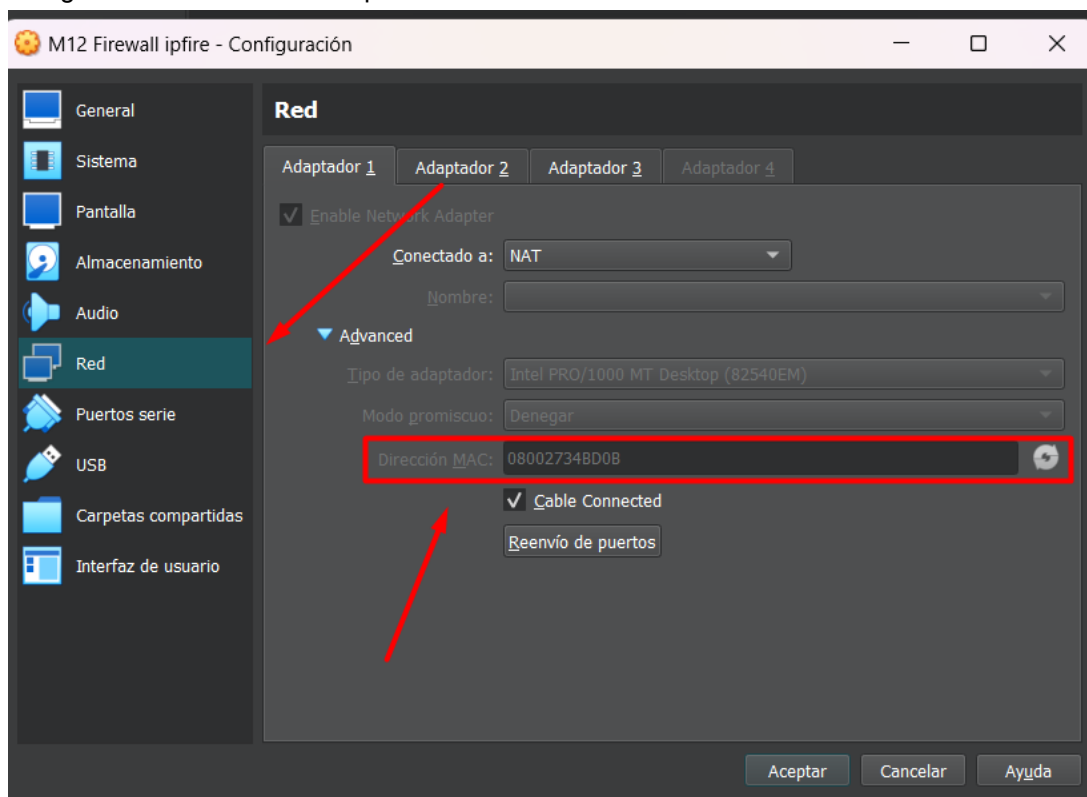
En este caso, se deberá seleccionar la segunda opción, que contiene las redes GREEN (red interna), RED(internet) y ORANGE (DMZ).



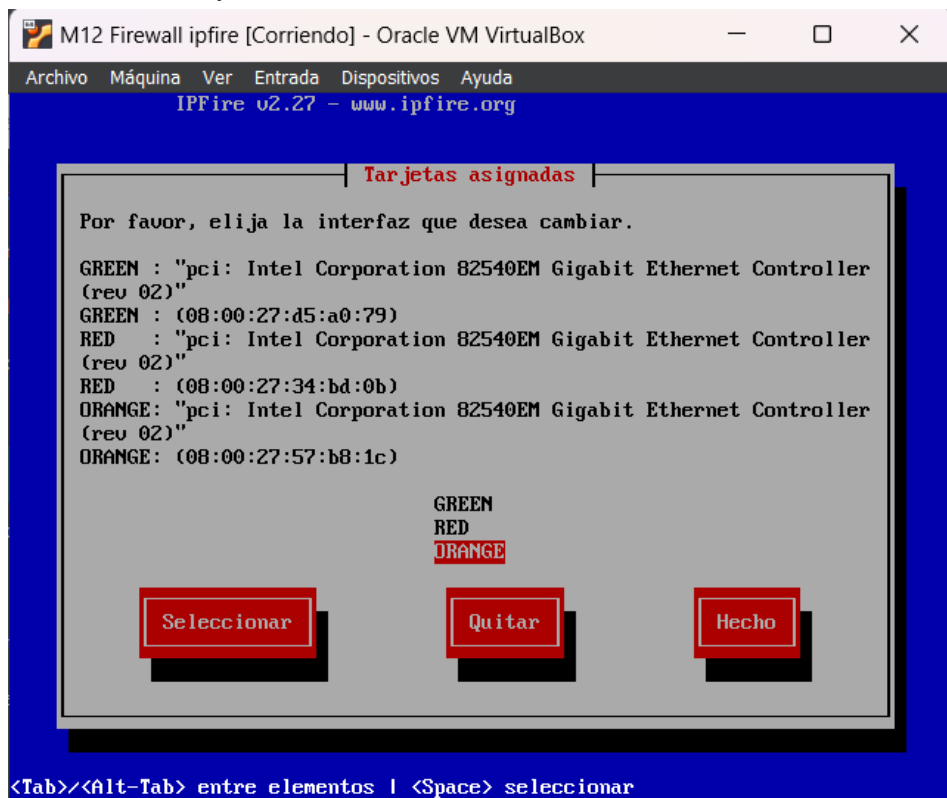
Acto seguido se le asignará a cada red una interfaz de red diferente, esto se hará consultando las direcciones MAC de los diferentes adaptadores.



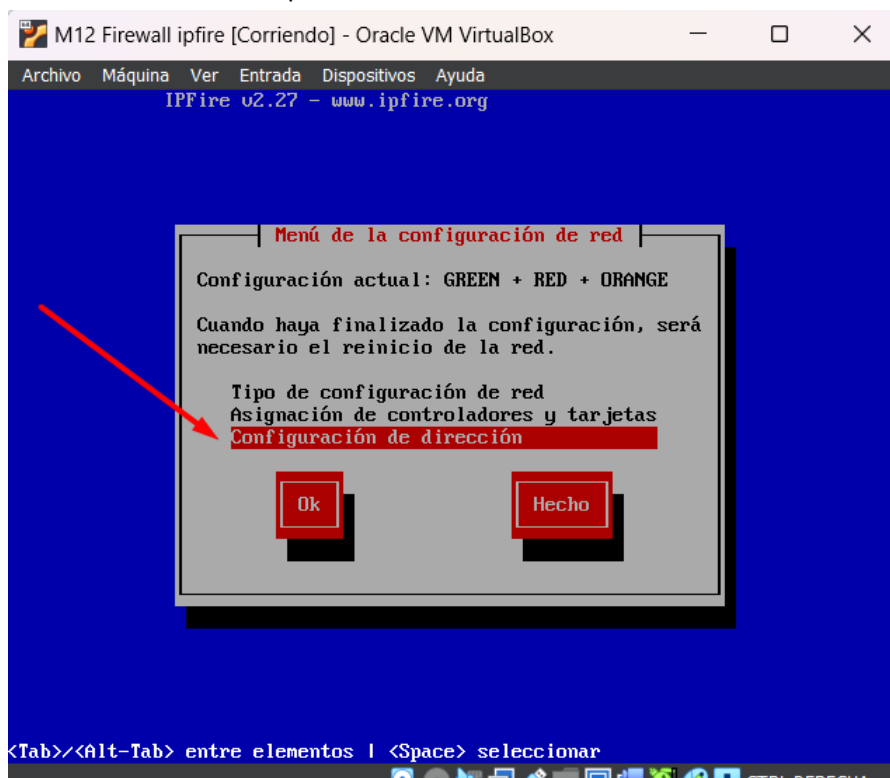
Se deberá consultar la MAC de cada una de las interfaces de red. En este caso, al hacerse en máquinas virtuales con VirtualBox se deberá consultar la MAC de cada una de las interfaces desde la configuración de red de la máquina en VirtualBox.



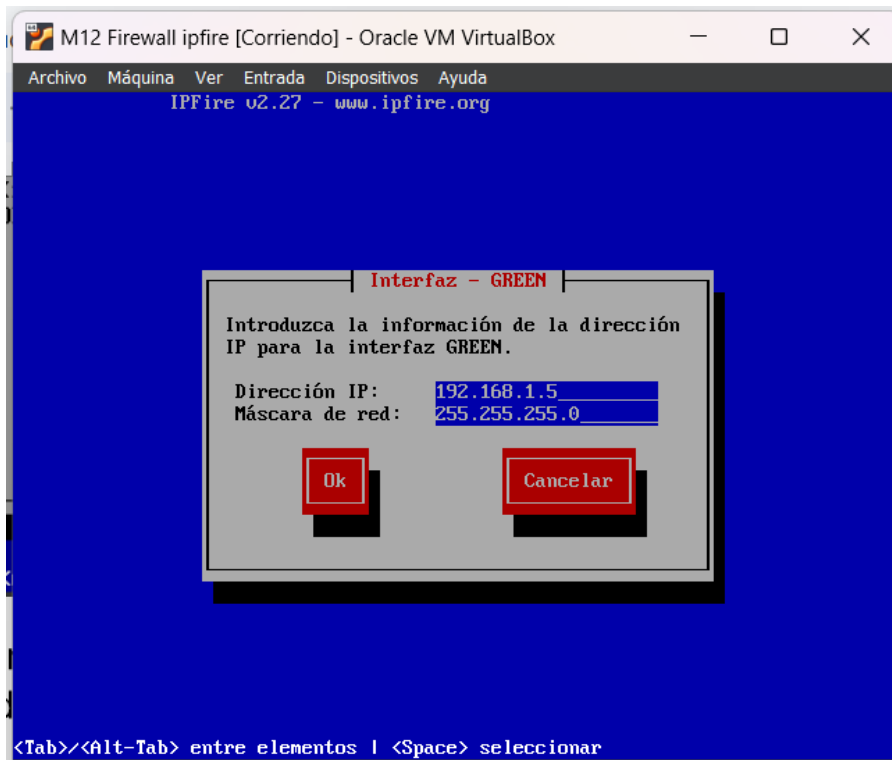
Una vez se tenga claro qué dirección MAC tiene cada uno de los adaptadores, se le deberá asignar una de las redes, ya sea GREEN, RED u ORANGE.



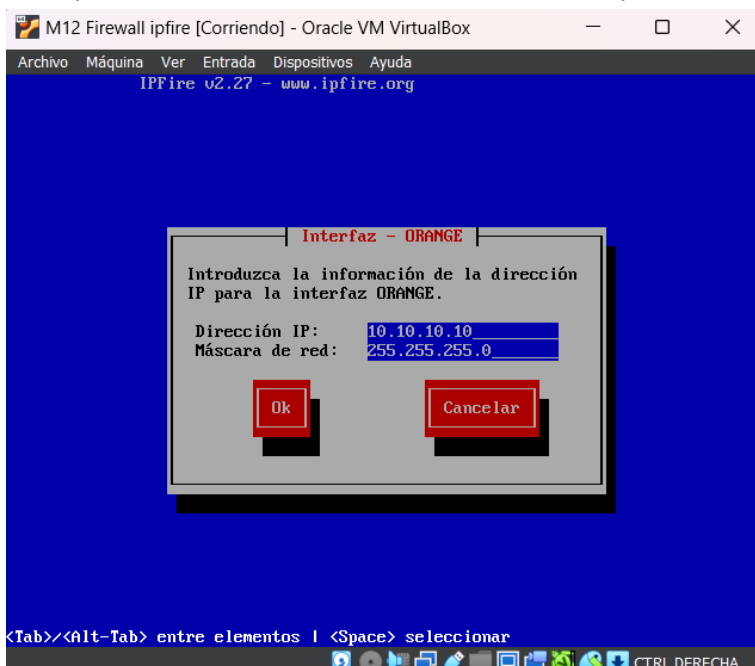
Por último, se deberán reconfigurar las redes para asignar a cada uno de los adaptadores una IP. Se deberá tener en cuenta que se trata de tres redes distintas, las cuales tendrán tres IPs diferentes.



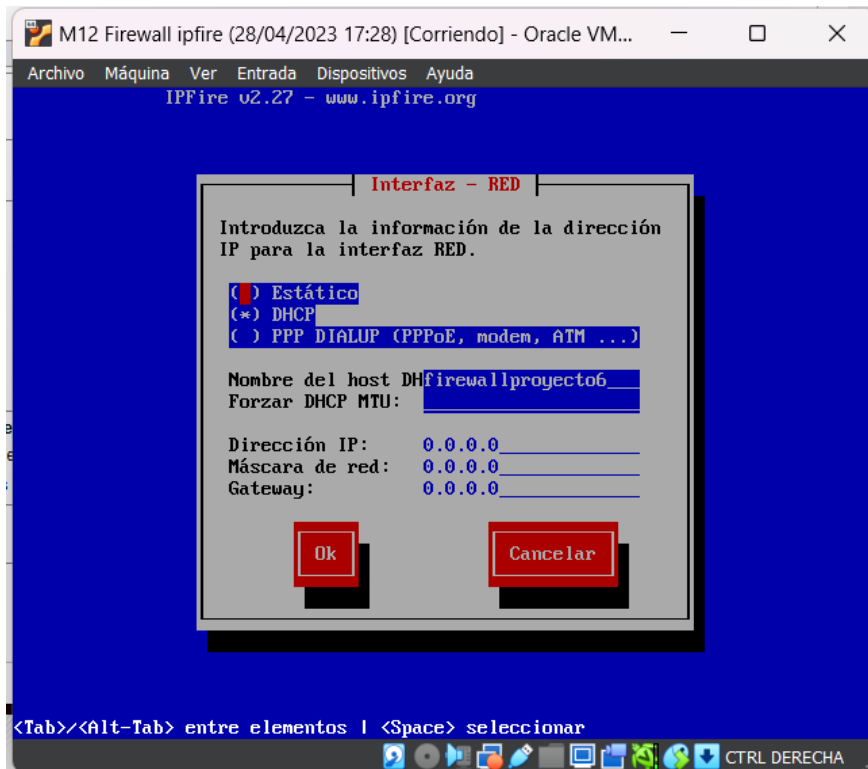
Al acceder a la red GREEN, se deberá especificar la IP del firewall dentro de la red interna. En este caso se utilizó una IP dentro del rango de la red interna, siendo esta una 192.168.1.5/24



En la configuración de la red ORANGE, se ha utilizado la IP 10.10.10.10 para este adaptador de red, haciendo que la DMZ donde van a ir instalados los servicios a los que se tendrá acceso desde la red externa (Internet), se encuentren en una red distinta a la red privada de la empresa, haciendo así que no se pueda acceder desde internet a la red interna pero sí al servidor web.



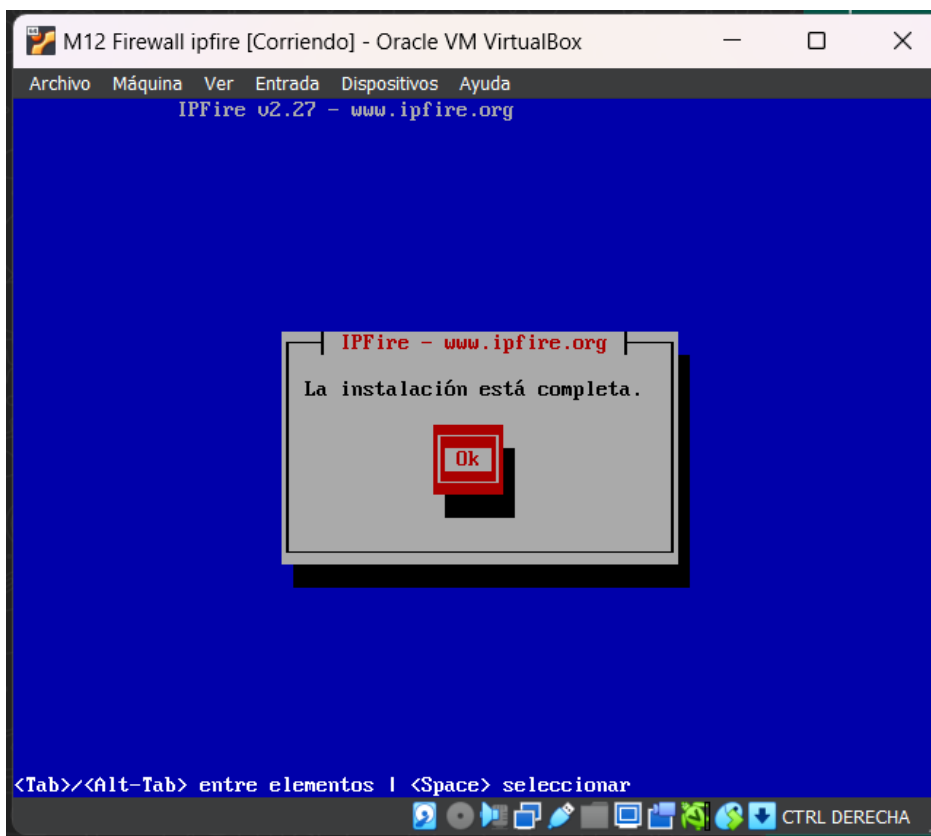
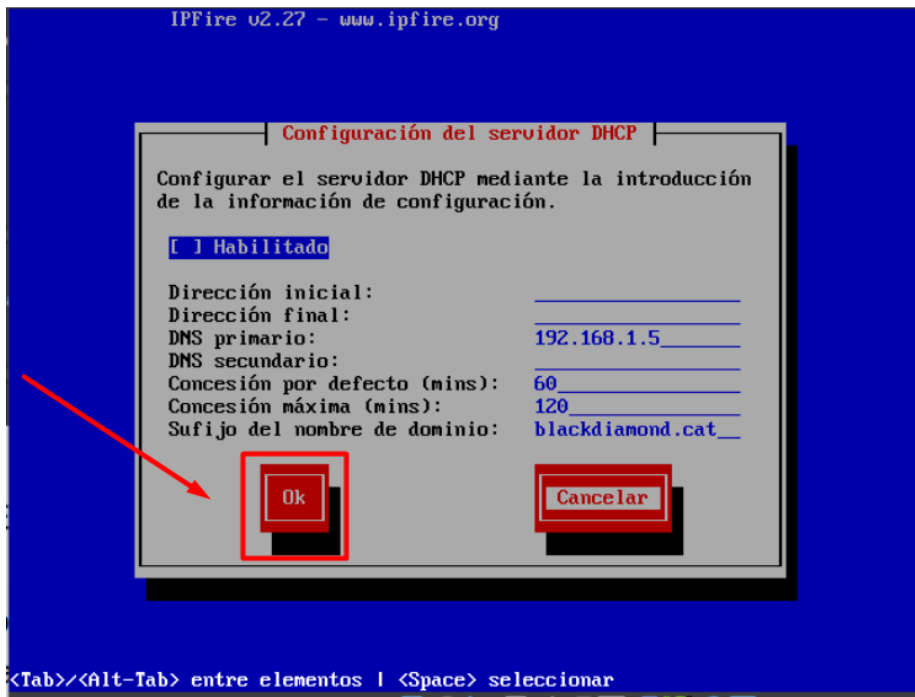
En la interfaz de la RED, pusimos la configuración de red a través del DHCP. Posteriormente, se deberá configurar para que se pueda acceder desde la red GREEN y ORANGE a la red RED, haciendo que todos tengan acceso a internet, pero desde la red RED (Internet) no se podrá acceder a la red GREEN, dando esto más seguridad a la red privada de la empresa.



Una vez se encuentre todo configurado se le dará al botón de hecho y se guardará la configuración de nuestro firewall.



Se nos pedirá la configuración del DHCP, en el caso de esta empresa ya se encuentra activo un servidor DHCP propio, por lo que no se deberá habilitar esta opción.



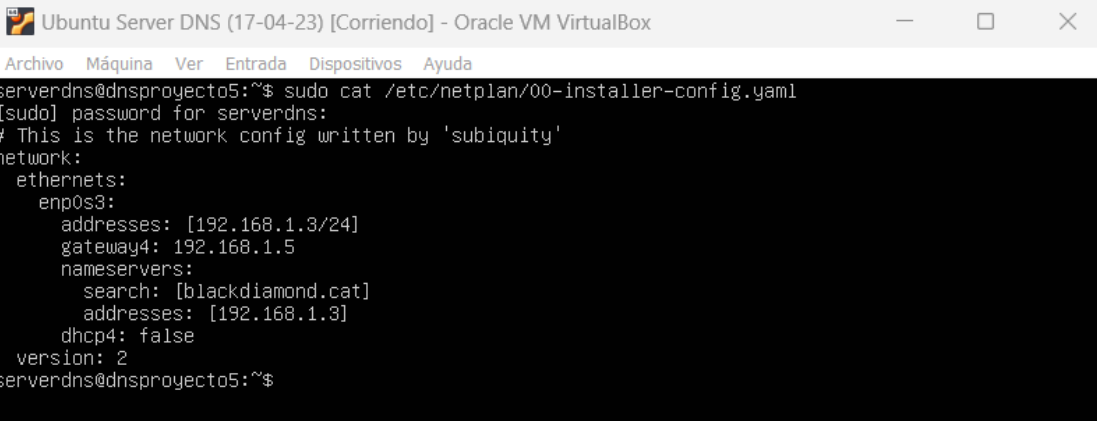
Una vez configurado el firewall se deberá comprobar que se encuentren aplicados todos los cambios de la configuración. Se utilizará el comando "ip a", para ver las IPs de todas las interfaces.

```
[root@firewallproyecto6 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: red0: <BROADCAST,UP,LOWER_UP> mtu 1500 qdisc cake state UP group default qlen 1000
    link/ether 08:00:27:34:bd:0b brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute red0
        valid_lft 82543sec preferred_lft 71743sec
3: green0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc cake state UP group default qlen 1000
    link/ether 08:00:27:d5:a0:79 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.5/24 scope global green0
        valid_lft forever preferred_lft forever
4: orange0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc cake state UP group default qlen 1000
    link/ether 08:00:27:57:b8:1c brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.10/24 scope global orange0
        valid_lft forever preferred_lft forever
[root@firewallproyecto6 ~]#
```

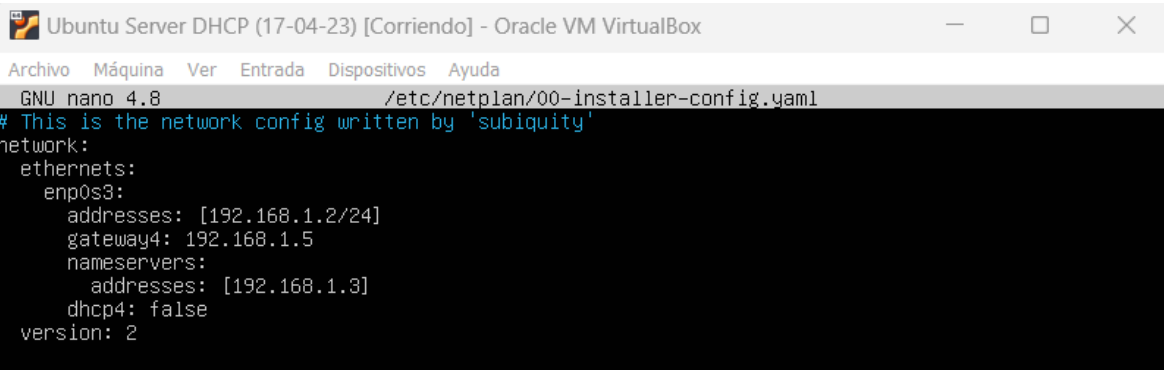
Al utilizar un "ip a" y ver que todas las interfaces de red se encuentran correctamente configuradas, se hará un ping a la IP 8.8.8.8 para comprobar que se tiene salida al exterior de la red.

```
[root@firewallproyecto6 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=23.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=20.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=119 time=19.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=119 time=23.1 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=119 time=20.6 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=119 time=22.9 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=119 time=23.7 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=119 time=21.2 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=119 time=22.7 ms
64 bytes from 8.8.8.8: icmp_seq=10 ttl=119 time=18.0 ms
64 bytes from 8.8.8.8: icmp_seq=11 ttl=119 time=26.2 ms
^X64 bytes from 8.8.8.8: icmp_seq=12 ttl=119 time=17.6 ms
64 bytes from 8.8.8.8: icmp_seq=13 ttl=119 time=19.5 ms
^C
--- 8.8.8.8 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12023ms
rtt min/avg/max/mdev = 17.600/21.447/26.246/2.375 ms
[root@firewallproyecto6 ~]#
```

Una vez tenemos la máquina de IPfire configurada, tendremos que cambiar en los archivos de configuración de los servidores DHCP y DNS, que el gateway sea el IPfire (192.168.1.5).



```
Ubuntu Server DNS (17-04-23) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
serverdns@dnsproyecto5:~$ sudo cat /etc/netplan/00-installer-config.yaml
[sudo] password for serverdns:
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses: [192.168.1.3/24]
      gateway4: 192.168.1.5
      nameservers:
        search: [blackdiamond.cat]
        addresses: [192.168.1.3]
      dhcp4: false
  version: 2
serverdns@dnsproyecto5:~$
```



```
Ubuntu Server DHCP (17-04-23) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 4.8 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      addresses: [192.168.1.2/24]
      gateway4: 192.168.1.5
      nameservers:
        addresses: [192.168.1.3]
      dhcp4: false
  version: 2
```

Y en el DHCP, tenemos que editar el archivo de configuración del servicio y cambiar la dirección del router que teníamos previamente configurada, por la ip de nuestro servidor ipfire.

```

GNU nano 4.8 /etc/dhcp/dhcpd.conf

# You can declare a class of clients and then do address allocation
# based on that.  The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

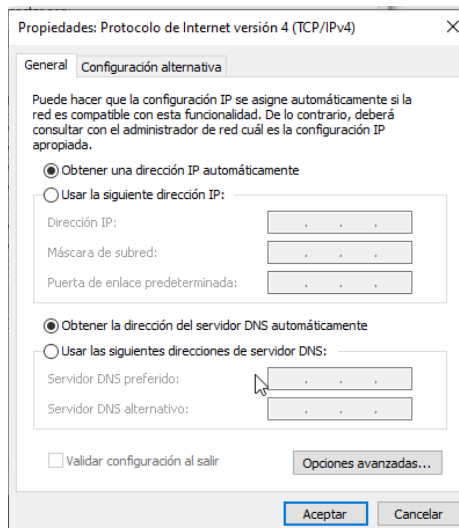
#class "foo" {
#  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}

subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.30 192.168.1.200;
  option routers 192.168.1.5;
  option domain-name-servers 192.168.1.3;
}

```

Una vez cambiado los archivos necesarios en los servidores, tendremos que abrir nuestro cliente GREEN y haremos el comando "ipconfig /renew" y nos deberá de dar como gateway la dirección 192.168.1.5, que es la dirección de nuestro servidor IPfire:



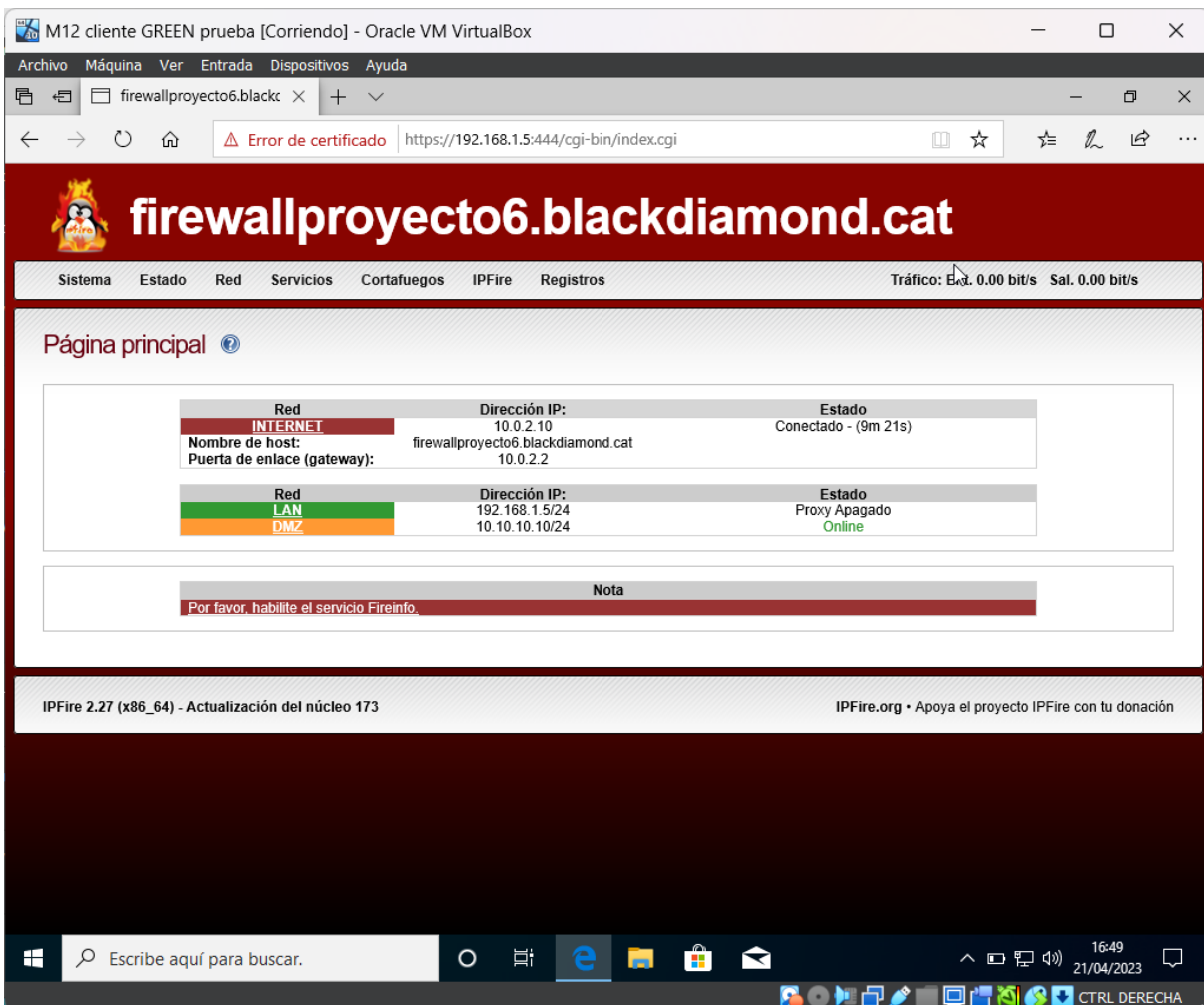
```
C:\Users\David>ipconfig /renew

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

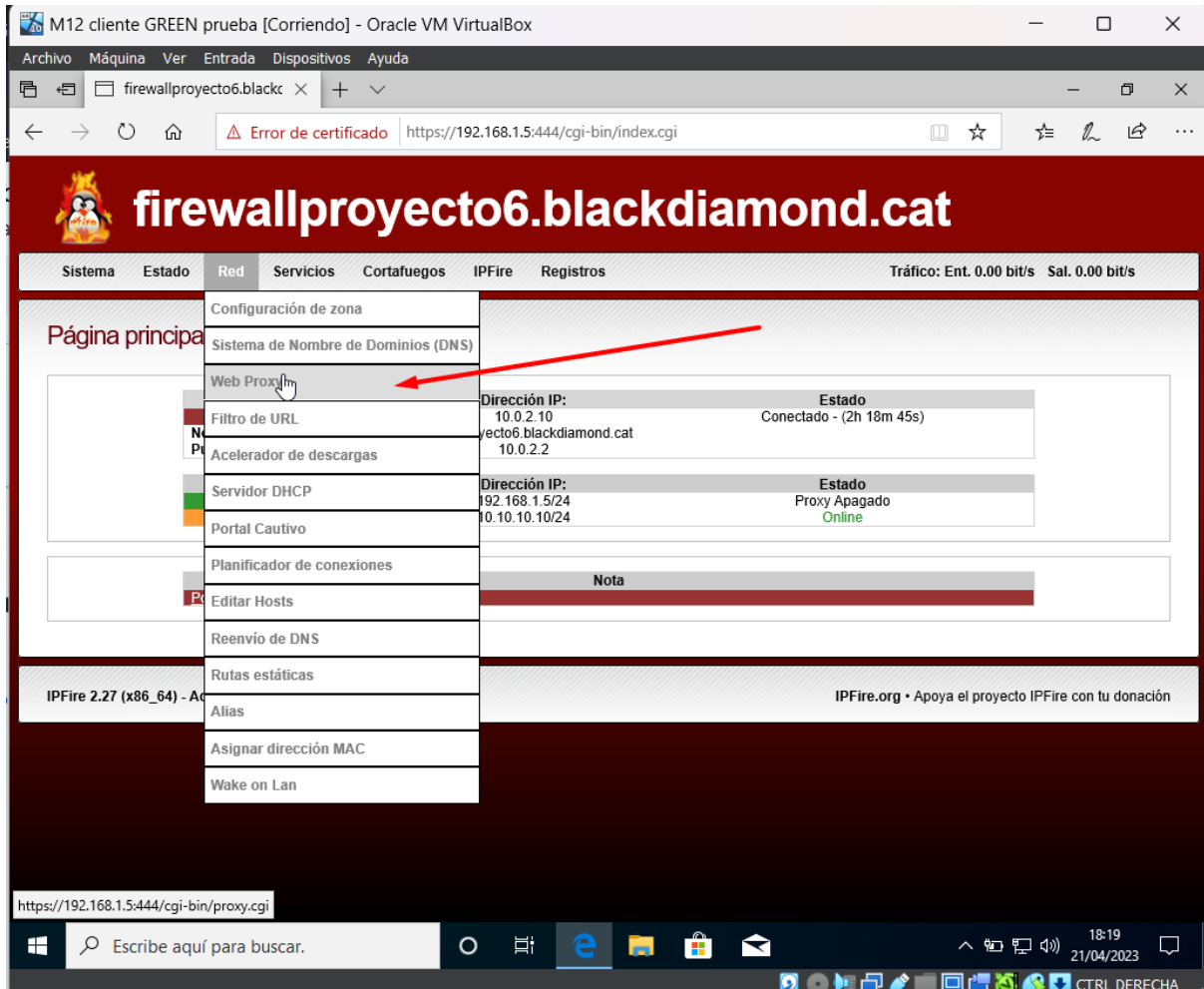
    Sufijo DNS específico para la conexión. . . : example.org
    Vínculo: dirección IPv6 local. . . . . : fe80::bc19:8b86:9fb5:65de%4
    Dirección IPv4. . . . . : 192.168.1.32
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.5
```

Ahora, desde el cliente de la red GREEN se accede a la página de configuración del firewall IPFire desde su entorno web. Simplemente, al acceder a un cliente se deberá poner la IP del firewall https://192.168.1.5:444, el puerto 444 es el que utiliza IPFire por defecto. Al acceder a esta IP debería salir la siguiente interfaz web.



2- Configuració d'un proxy que limiti el contingut al que poden accedir els equips de la xarxa

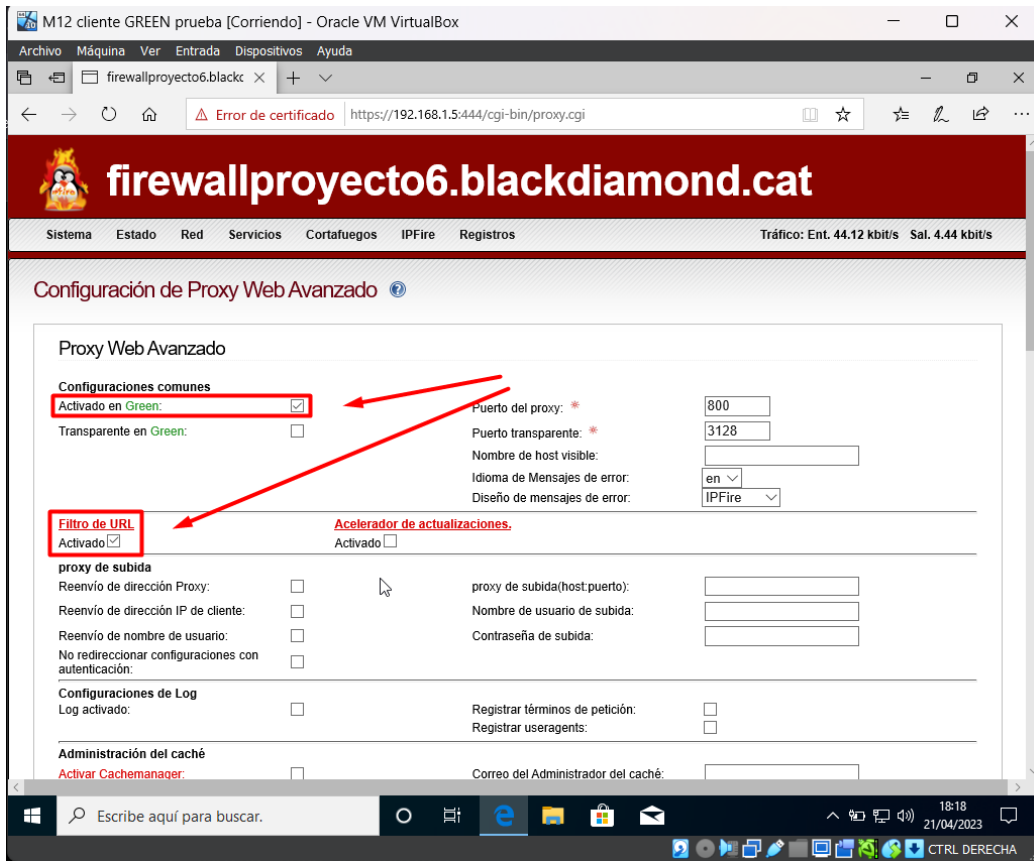
Una vez se tenga acceso a IPFire, se configurará el Proxy y sus respectivos filtros. Se deberá acceder al apartado de "Red" y se seleccionará "Web Proxy".



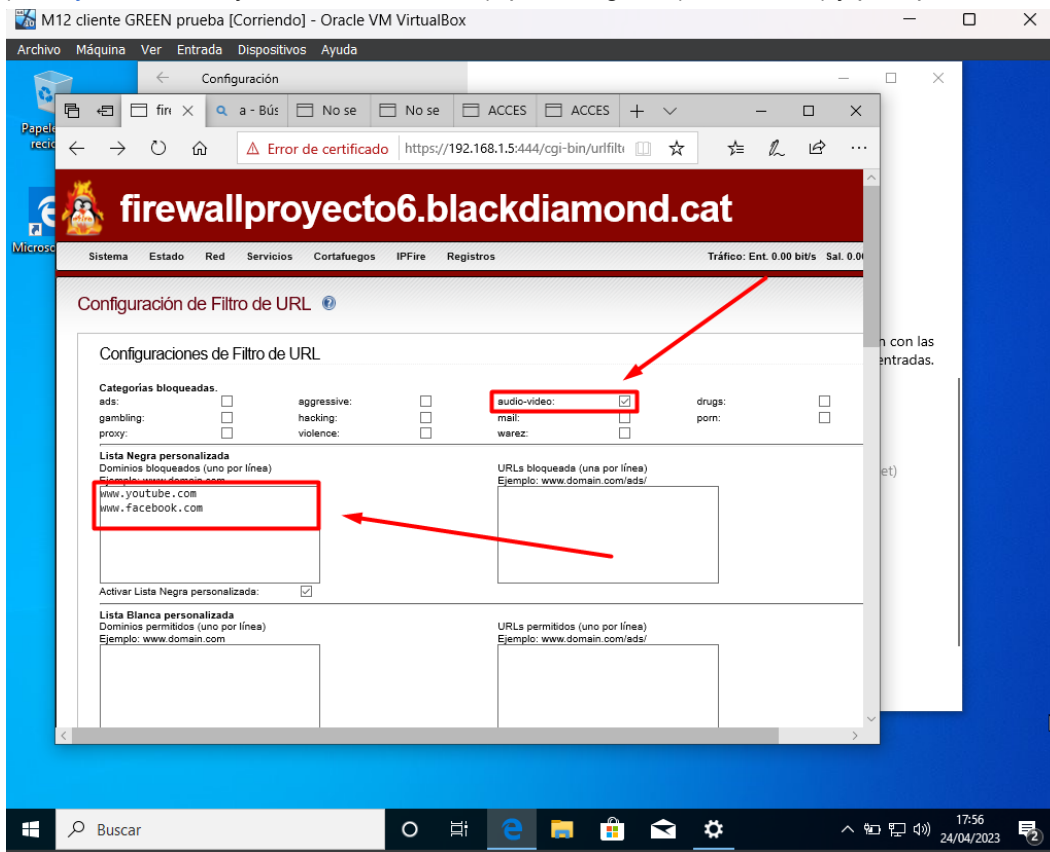
The screenshot shows the IPFire web interface in a browser window. The browser address bar shows a certificate error for the URL `https://192.168.1.5:444/cgi-bin/index.cgi`. The main content area displays the 'Web Proxy' configuration page, which is highlighted by a red arrow. The page includes a sidebar with various configuration options and a main content area with a table of proxy settings.

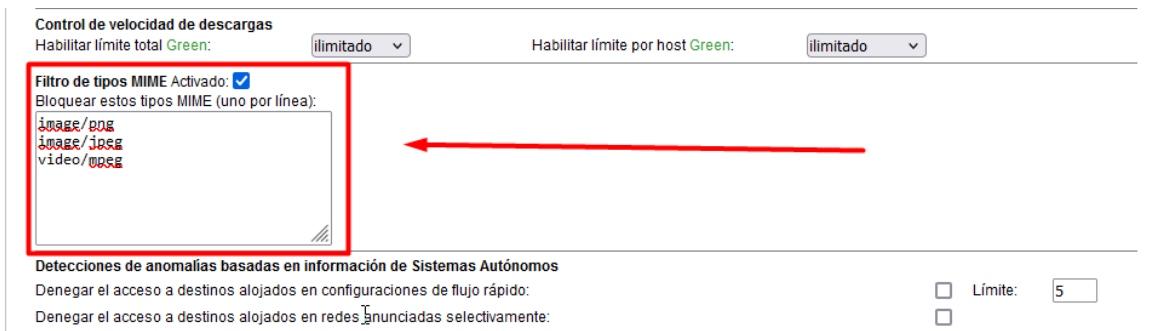
Dirección IP:	Estado
10.0.2.10	Conectado - (2h 18m 45s)
192.168.1.5/24	Proxy Apagado
10.10.10.10/24	Online

Una vez se acceda a dicho apartado, se deberán activar las siguientes opciones:

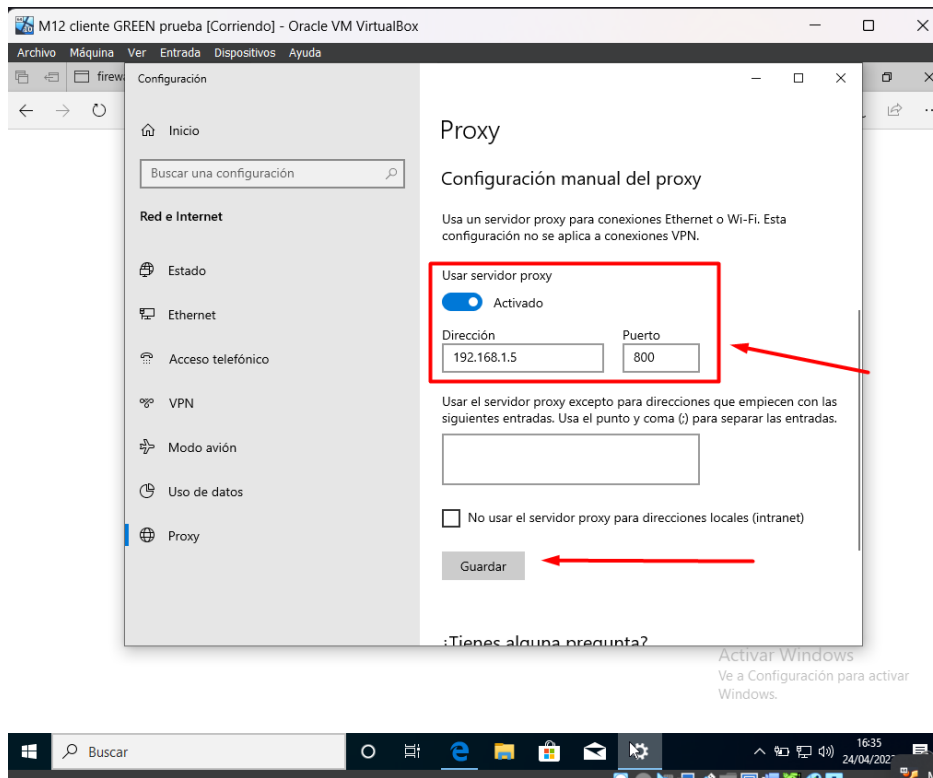


Dentro del filtrado por URL, se especificarán tres formas diferentes de filtraje, por dominio (www.youtube.com y www.facebook.com), por categoría (audio-video) y por tipos MIME.



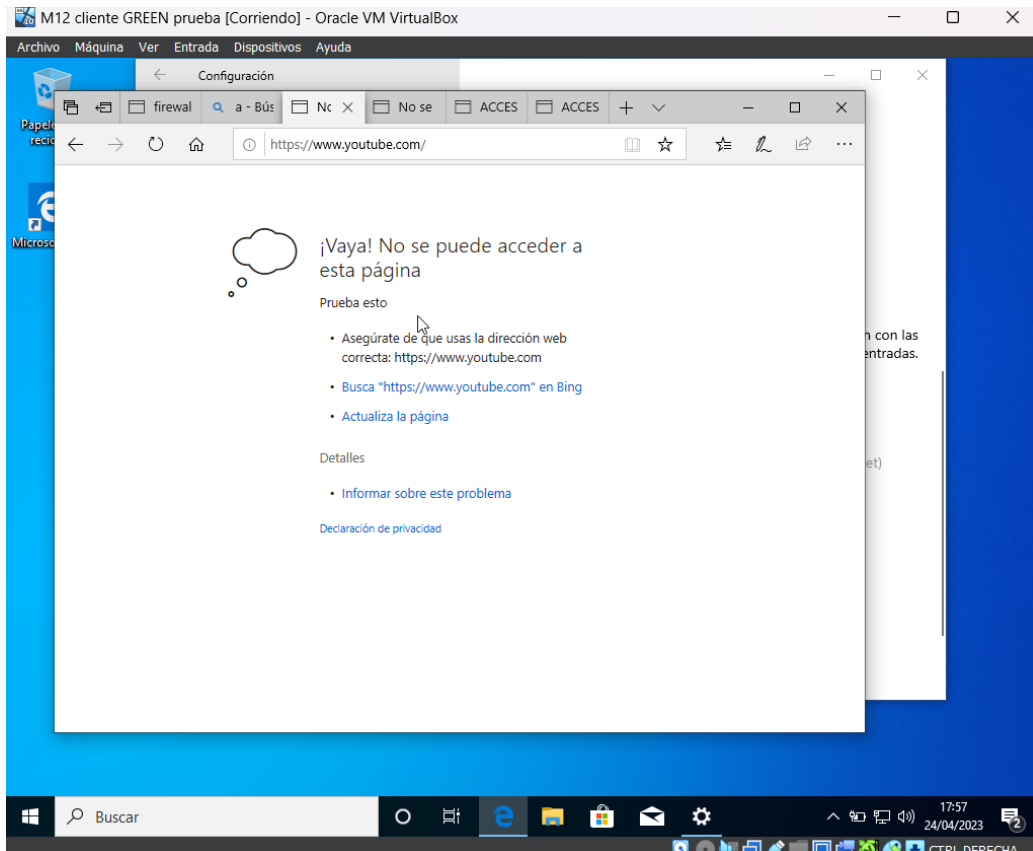


Se añadirá la configuración del proxy en los clientes Windows.

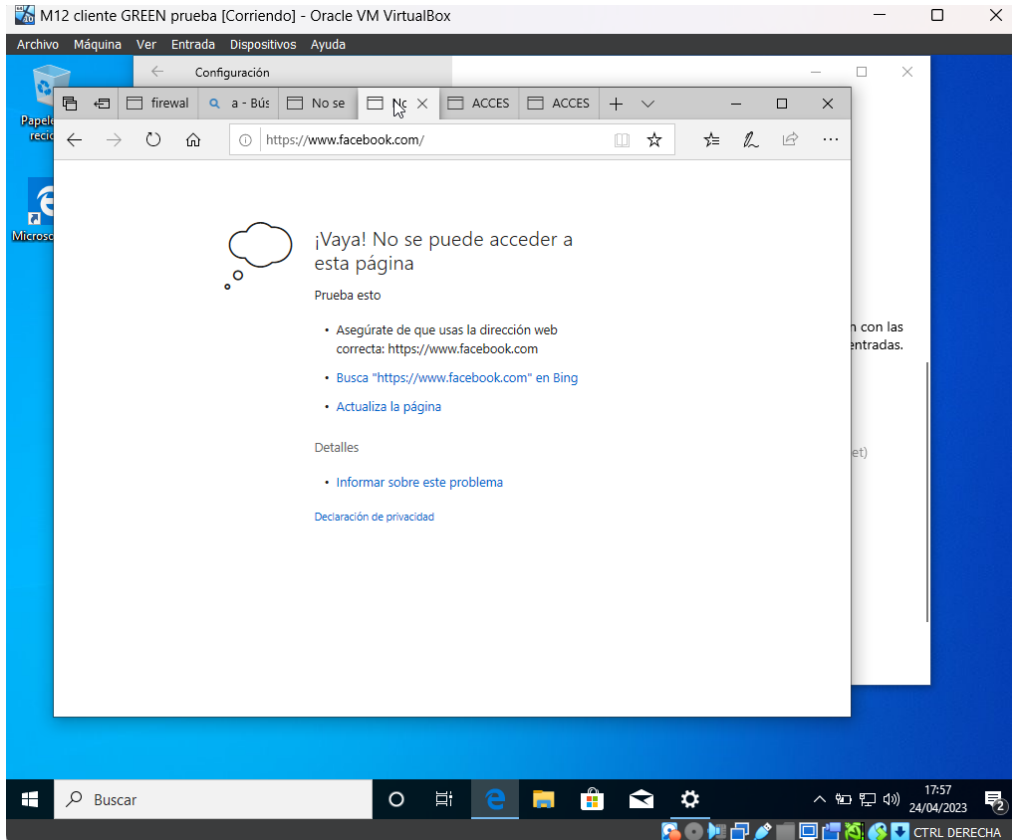


Al intentar acceder a las páginas que se encuentren bloqueadas saldrá el siguiente mensaje de error:

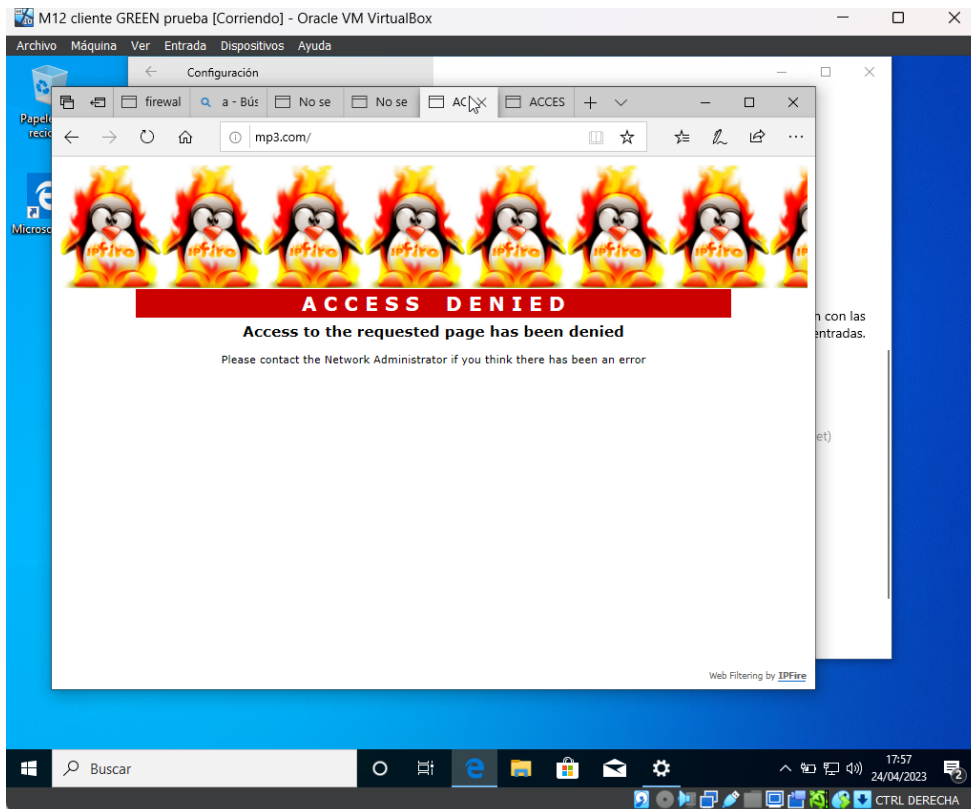
[www.youtube.com:](https://www.youtube.com/)



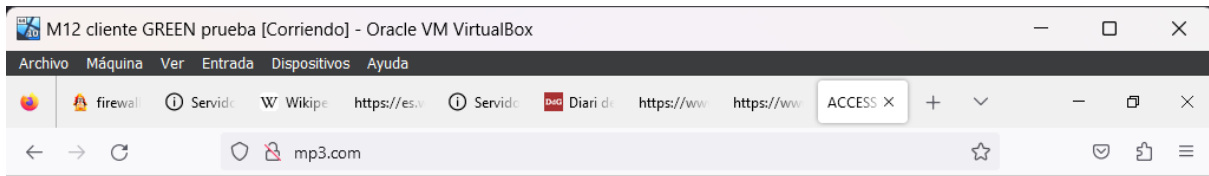
[www.facebook.com:](https://www.facebook.com/)



Todas las páginas que se encuentren dentro de la categoría audio-video:



Y el filtraje de MIME, bloquea las imágenes de, por ejemplo, el aviso que nos salía antes con imágenes en el IPFire, con el filtro activo, no se muestran.



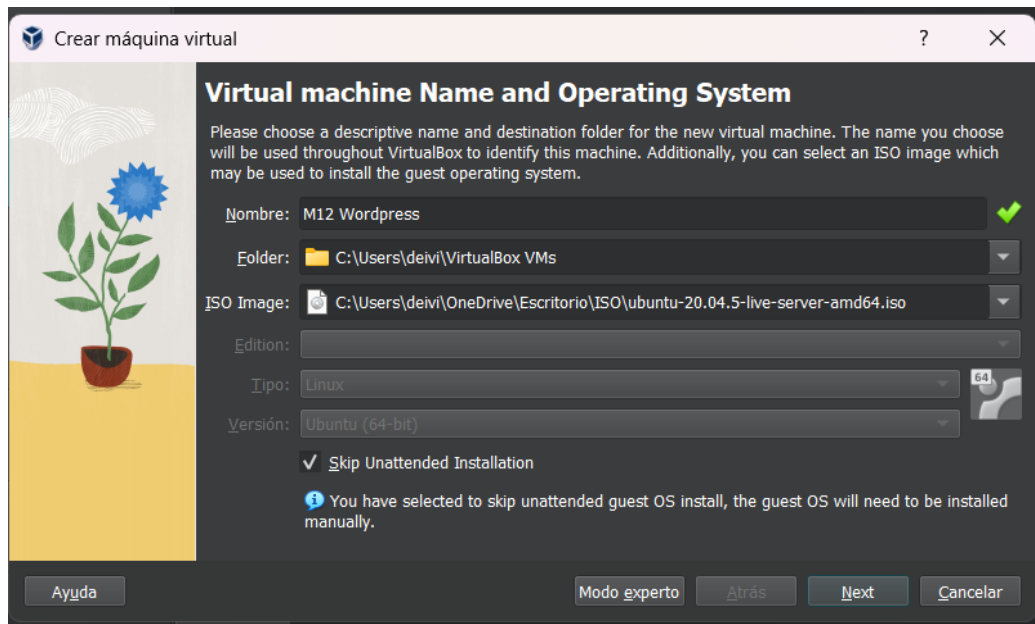
ACCESS DENIED
Access to the requested page has been denied
Please contact the Network Administrator if you think there has been an error



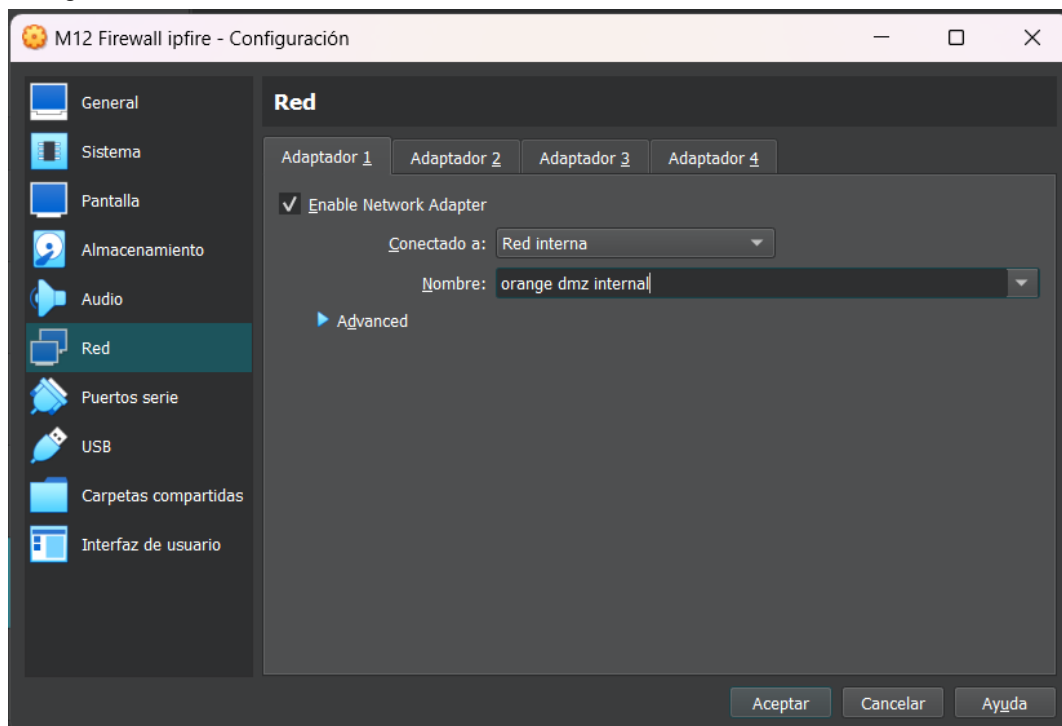
Fase 2 – Migració Wordpress on-premise

1- Selecció del sistema operatiu i serveis que habilitareu per a poder migrar l'actual wordpress que teniu allotjat al núvol cap a una infraestructura on premise (hosting).

Crearem una màquina virtual de Ubuntu Server 20.04, donde migrarem nostra pàgina de Wordpress del Proyecto 4:



Cambiarem dentro del VirtualBox la configuració de red i la connectarem a la red interna Orange.



Dentro de la máquina virtual, tendremos que instalar el apache2.

```

wordpress@wordpressprojecto6:~$ sudo service apache2 status
• apache2.service - The Apache HTTP Server
  Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Active: active (running) since Fri 2023-05-05 15:36:26 UTC; 6min ago
  Docs: https://httpd.apache.org/docs/2.4/
  Main PID: 16698 (apache2)
  Tasks: 55 (limit: 4609)
  Memory: 5.2M
  CGroup: /system.slice/apache2.service
          └─16698 /usr/sbin/apache2 -k start
            └─16700 /usr/sbin/apache2 -k start
              └─16701 /usr/sbin/apache2 -k start

may 05 15:36:26 wordpressprojecto6 systemd[1]: Starting The Apache HTTP Server...
may 05 15:36:26 wordpressprojecto6 apachectl[16677]: AH00558: apache2: Could not reliably determine
may 05 15:36:26 wordpressprojecto6 systemd[1]: Started The Apache HTTP Server.
lines 1-15/15 (END)

```

Y probamos a entrar a la web por defecto de apache, accediendo a través de la ip de la máquina (usaremos una interfaz “HOST-ONLY” para acceder fácilmente desde la máquina real).

Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```

/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.Load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf

```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Ahora tenemos que instalar el servicio PHP, y seguidamente tenemos que instalar algunos módulos que serán útiles para el servicio.

```
wordpress@wordpressproyecto6:~$ sudo apt -y install php
```

```
wordpress@wordpressproyecto6:~$ sudo apt -y install php-mysql php-curl php-gd php-zip
```

Verificamos la instalación con este comando para ver la versión que se ha instalado.

```
wordpress@wordpressproyecto6:~$ php -v
PHP 7.4.3-4ubuntu2.18 (cli) (built: Feb 23 2023 12:43:23) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
with Zend OPcache v7.4.3-4ubuntu2.18, Copyright (c), by Zend Technologies
```

Reiniciamos el servicio de apache.

```
wordpress@wordpressproyecto6:~$ sudo systemctl restart apache2
```

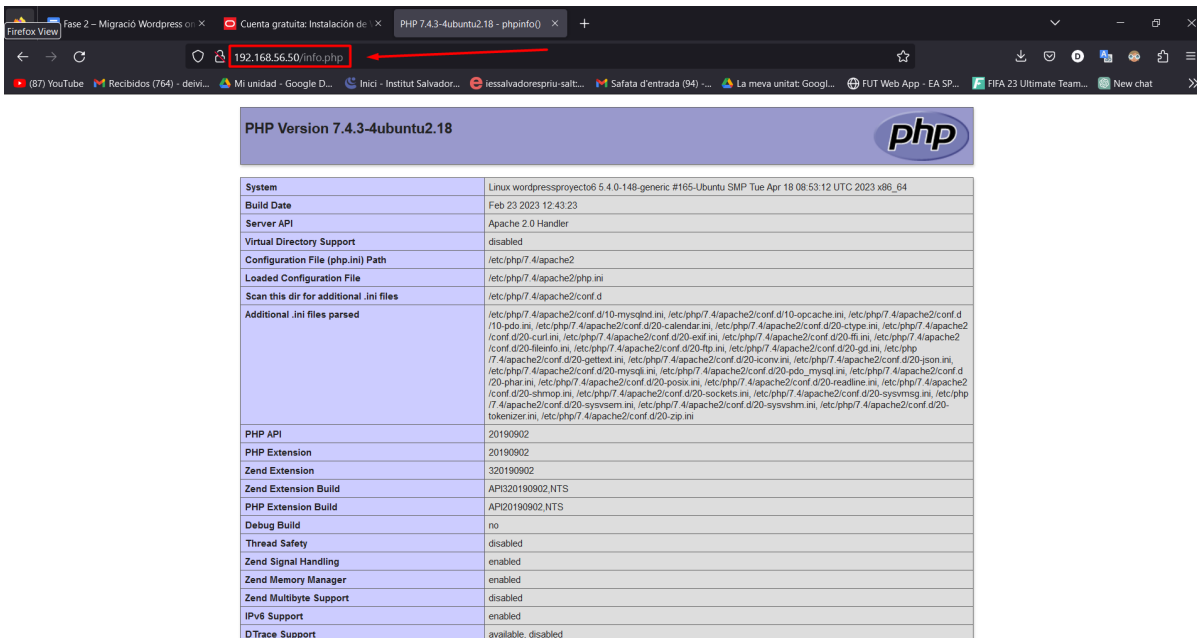
Creamos el archivo "info.php" en el directorio /var/www/html/.

```
wordpress@wordpressproyecto6:~$ sudo nano /var/www/html/info.php
```

Y seguidamente modificamos el archivo añadiendo las tres líneas que aparecen en la captura inferior.

```
GNU nano 4.8 /var/www/html/info.php Modified
<?php
phpinfo();
?>
```

Ahora si nos conectamos a <http://dirección IP del servidor/info.php>. Nos generará una lista de la configuración de PHP en la máquina virtual, como la siguiente:



PHP Version 7.4.3-4ubuntu2.18	
System	Linux wordpressproyecto6 5.4.0-148-generic #165-Ubuntu SMP Tue Apr 18 08:53:12 UTC 2023 x86_64
Build Date	Feb 23 2023 12:43:23
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-curl.ini, /etc/php/7.4/apache2/conf.d/20-enchant.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gd.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mysql.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysmsg.ini, /etc/php/7.4/apache2/conf.d/20-sysvsem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini, /etc/php/7.4/apache2/conf.d/20-zip.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS
PHP Extension Build	API20190902.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled

Esto nos sirvió para probar que el servicio está funcionando correctamente, ahora se puede borrar el archivo creado.

```
wordpress@wordpressproyecto6:~$ sudo rm /var/www/html/info.php
```

Ahora, crearemos un usuario que esté dentro del grupo **www-data**.

```
wordpress@wordpressproyecto6:~$ sudo adduser wordpress www-data
Adding user `wordpress' to group `www-data' ...
Adding user wordpress to group www-data
Done.
```

Cambiamos el propietario de la carpeta `/var/www/html`.

```
wordpress@wordpressproyecto6:~$ sudo chown -R www-data:www-data /var/www/html
```

Cambiamos los permisos de la carpeta `/var/www/html` a los siguientes:

```
wordpress@wordpressproyecto6:~$ sudo chmod -R g+rw /var/www/html
```

Vemos que se han cambiado los permisos de la carpeta.

```
wordpress@wordpressproyecto6:~$ sudo ls -l /var/www/html
total 12
-rw-rw-r-- 1 www-data www-data 10918 may  5 15:36 index.html
```

Instalamos el paquete de MySQL.

```
wordpress@wordpressproyecto6:~$ sudo apt -y install mysql-server
```

Una vez instalado en MySQL, iniciamos sesión.

```
wordpress@wordpressproyecto6:~$ sudo mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 8.0.32-0ubuntu0.20.04.2 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Cambiamos el usuario MySQL "root" para permitirnos la autenticación de contraseña.

```
mysql> ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password by '1234';
Query OK, 0 rows affected (0,07 sec)
```

Ahora tenemos que proteger MySQL con el script siguiente:

```
wordpress@wordpressproyecto6:~$ sudo mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root:

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: y

There are three levels of password validation policy:

LOW      Length >= 8
MEDIUM  Length >= 8, numeric, mixed case, and special characters
STRONG  Length >= 8, numeric, mixed case, special characters and dictionary
         file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 0
Using existing password for root.
```

Nos pedirá la contraseña que hemos puesto previamente, y seguidamente tenemos activar la validación por contraseña, seleccionamos “y” para decir que “sí”, escogemos el nivel de validación y cambiamos y definimos la contraseña de raíz.

```
Estimated strength of the password: 25
Change the password for root ? ((Press y|Y for Yes, any other key for No) : y

New password:

Re-enter new password:

Estimated strength of the password: 50
Do you wish to continue with the password provided?(Press y|Y for Yes, any other
key for No) : y
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.
```

Ahora seleccionamos las demás opciones de seguridad confirmando con “y” y denegar con cualquier otra.


```
Remove anonymous users? (Press y|Y for Yes, any other key for No) : y
Success.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : n

... skipping.
By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No)
: y
- Dropping test database...
Success.

- Removing privileges on test database...
Success.

Reloading the privilege tables will ensure that all changes
made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y
Success.

All done!
```

Seguidamente, tenemos que iniciar sesión en el MySQL con la nueva contraseña puesta anteriormente.

```
wordpress@wordpressproyecto6:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 20
Server version: 8.0.32-0ubuntu0.20.04.2 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Ahora tenemos que volver a cambiar el método de autenticación MySQL a "auth_socket", y una vez hecho salimos del MySQL.

```
mysql> ALTER USER 'root'@'localhost' IDENTIFIED WITH auth_socket;
Query OK, 0 rows affected (0,02 sec)
```

```
mysql> exit
```

Ahora para configurar la base de datos del wordpress del MySQL, primeramente tenemos que iniciar sesión en el MySQL.

```
wordpress@wordpressproyecto6:~$ sudo mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 21
Server version: 8.0.32-0ubuntu0.20.04.2 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Ahora tenemos que mostrar las bases de datos por defecto.

```
mysql> show databases;
+-----+
| Database                |
+-----+
| information_schema      |
| mysql                   |
| performance_schema     |
| sys                     |
+-----+
4 rows in set (0,01 sec)
```

Creamos un usuario para el MySQL, y le damos privilegios de administrador.

```
mysql> CREATE USER 'wordpress'@'localhost' IDENTIFIED BY '12345678';
Query OK, 0 rows affected (0,03 sec)

mysql>
```

```
mysql> GRANT ALL PRIVILEGES ON *.* TO 'wordpress'@'localhost';
Query OK, 0 rows affected (0,03 sec)
```

Creamos la base de datos WordPress.

```
mysql> create database wpdb;
Query OK, 1 row affected (0,09 sec)
```

Y seguidamente comprobamos que el resultado fue exitoso, viendo si se creó la base de datos.

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
| wpdb |
+-----+
5 rows in set (0,01 sec)
```

Vaciamos los privilegios para borrar la memoria caché, y seguidamente cerramos sesión en el MySQL.

```
mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,06 sec)

mysql> exit
Bye
```

Ahora descargamos el zip de WordPress Linux de https://es.wordpress.org/latest-es_ES y lo descomprimos (este comando crea un directorio "wordpress" con el código PHP para WordPress).

```
wordpress@wordpressproyecto6:~$ sudo wget https://es.wordpress.org/latest-es_ES.tar.gz
--2023-05-05 17:13:30-- https://es.wordpress.org/latest-es_ES.tar.gz
Resolving es.wordpress.org (es.wordpress.org)... 198.143.164.252
Connecting to es.wordpress.org (es.wordpress.org)|198.143.164.252|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 23803227 (23M) [application/octet-stream]
Saving to: 'latest-es_ES.tar.gz'

latest-es_ES.tar.gz 100%[=====>] 22,70M 1,60MB/s in 26s
2023-05-05 17:13:57 (889 KB/s) - 'latest-es_ES.tar.gz' saved [23803227/23803227]
```

```
wordpress@wordpressproyecto6:~$ tar xvfz latest-es_ES.tar.gz
```

Ahora copiamos el contenido del directorio WordPress (que se nos habrá creado previamente) en el directorio `/var/www/html`.

```
wordpress@wordpressproyecto6:~$ sudo cp -R wordpress/* /var/www/html
```

Ahora, si se quiere, se puede borrar el directorio WordPress, ya que se ha copiado a otro directorio.

```
wordpress@wordpressproyecto6:~$ sudo rm -r wordpress/
```

Aquí podemos comprobar que todo del archivo se ha copiado de manera exitosa dentro del directorio.

```
wordpress@wordpressproyecto6:~$ ls
latest-es ES.tar.gz
wordpress@wordpressproyecto6:~$ ls /var/www/html/
index.html      wp-admin          wp-cron.php      wp-mail.php
index.php       wp-blog-header.php wp-includes      wp-settings.php
license.txt     wp-comments-post.php wp-links-opml.php wp-signup.php
readme.html    wp-config-sample.php wp-load.php      wp-trackback.php
wp-activate.php wp-content        wp-login.php     xmlrpc.php
```

Ahora cambiamos al directorio `/var/www/html`.

```
wordpress@wordpressproyecto6:~$ cd /var/www/html
wordpress@wordpressproyecto6:/var/www/html$
```

Cambiamos el nombre del archivo “index.html” por defecto (esto hará que se cargue por defecto index.php cada vez que accedemos al directorio raíz).

```
mv: cannot move 'index.html' to 'index.html.bk': permission denied
wordpress@wordpressproyecto6:/var/www/html$ sudo mv index.html index.html.bk
```

Ahora cambiamos el nombre del archivo “wp-config-sample.php”.

```
wordpress@wordpressproyecto6:/var/www/html$ sudo mv wp-config-sample.php wp-config.php
```

Haremos “sudo nano wp-config.php” para editar el archivo de configuración del WordPress, y aquí, especificaremos nuestras credenciales de la base de datos.

```
wordpress@wordpressproyecto6:/var/www/html$ sudo nano wp-config.php
```

```
*/
// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wpdb' );

/** Database username */
define( 'DB_USER', 'wordpress' );

/** Database password */
define( 'DB_PASSWORD', '12345678' );
/** Database hostname */
```

Ahora, si accedemos a la dirección `https://dirección IP del servidor/wp-admin/install.php`, podremos ver que está en funcionamiento la página.

Fase 2 – Migración Instalación de WordPress Cuenta gratuita: wp-config.php

192.168.56.5/wp-admin/install.php

Hola

¡Este es el famoso proceso de instalación de WordPress en cinco minutos! Simplemente completa la información siguiente y estarás a punto de usar la más enriquecedora y potente plataforma de publicación personal del mundo.

Información necesaria

Por favor, proporciona la siguiente información. No te preocupes, siempre podrás cambiar estos ajustes más tarde.

Título del sitio

Nombre de usuario

Los nombres de usuario pueden tener únicamente caracteres alfanuméricos, espacios, guiones bajos, guiones medios, puntos y el símbolo @.

Contraseña

Fuerte

Importante: Necesitas esta contraseña para acceder. Por favor, guárdala en un lugar seguro.

Llenamos la información necesaria para terminar de instalar el WordPress y crear el usuario, tales como: el usuario, la contraseña, etc, y le damos a "Instalar WordPress".

Información necesaria

Por favor, proporciona la siguiente información. No te preocupes, siempre podrás cambiar estos ajustes más tarde.

Título del sitio

Nombre de usuario
 Los nombres de usuario pueden tener únicamente caracteres alfanuméricos, espacios, guiones bajos, guiones medios, puntos y el símbolo @.

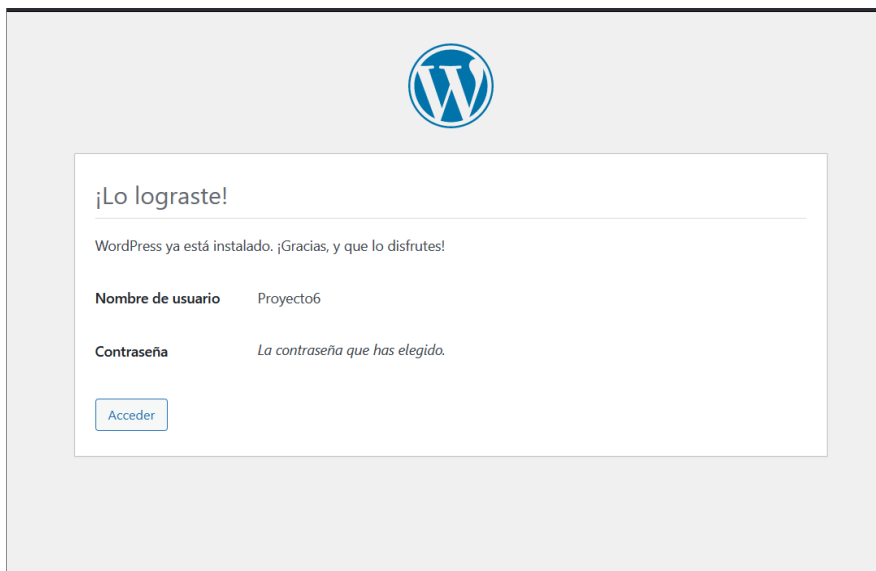
Contraseña
 Muy débil
Importante: Necesitas esta contraseña para acceder. Por favor, guárdala en un lugar seguro.

Confirma la contraseña Confirma el uso de una contraseña débil.

Tu correo electrónico
 Comprueba bien tu dirección de correo electrónico antes de continuar.

Visibilidad en los motores de búsqueda Pedir a los motores de búsqueda que no indexen este sitio
 Depende de los motores de búsqueda atender esta petición o no.

Como podemos ver, ya hemos logrado la creación del usuario de WordPress, y su instalación.



Lo siguiente que tendremos que hacer será añadir dentro del archivo de configuración de WordPress una línea para que no nos salte este error al instalar algún plug-in.

Datos de conexión

Fallo al conectar al servidor FTP 192.168.56.50:21

Para realizar la operación que has solicitado WordPress necesita tener acceso a tu servidor web. Por favor, introduce tus datos de acceso FTP para proceder. Si no recuerdas tus datos de acceso deberías contactar con tu proveedor de alojamiento.

Hostname
ejemplo: es.wordpress.org

Usuario FTP
Proyecto6

Contraseña FTP
••••

Esta contraseña no se almacenará en el servidor.

Tipo de conexión
 FTP
 FTPS (SSL)

Cancelar Ejecutar

La línea que tendremos que añadir en este documento.

```
wordpress@wordpressproyecto6:~$ sudo nano /var/www/html/wp-config.php
```

será esta: **define('FS_METHOD','direct');**

```
GNU nano 4.8 /var/www/html/wp-config.php Modified
* @link https://wordpress.org/documentation/article/editing-wp-config-php/
*
* @package WordPress
*/

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('FS_METHOD','direct');
define( 'DB_NAME', 'wpdb' );

/** Database username */
define( 'DB_USER', 'wordpress' );

/** Database password */
define( 'DB_PASSWORD', '12345678' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

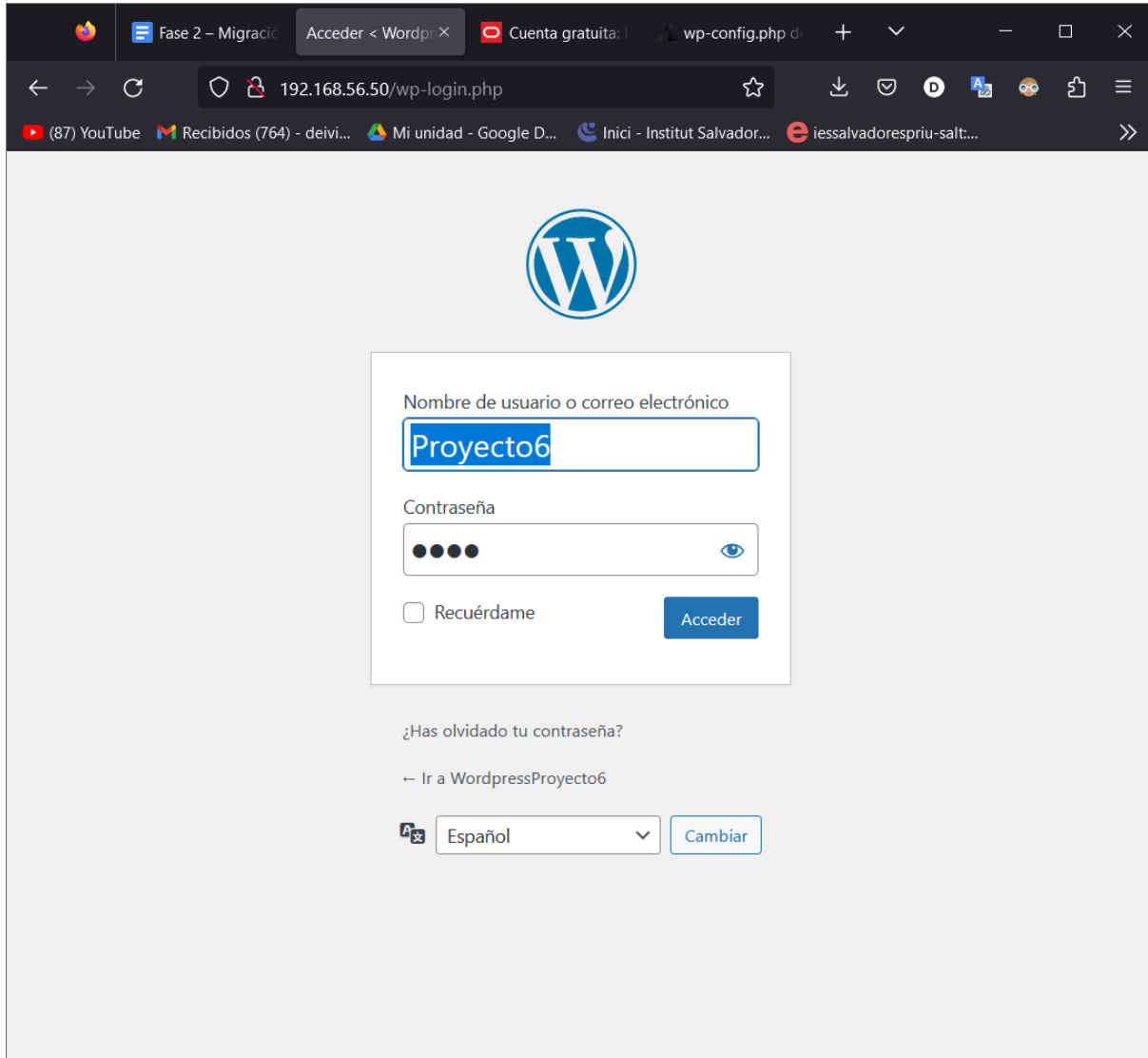
También aprovecharemos y cambiaremos los permisos de la carpeta “**/var/www/html**” con este comando:

```
wordpress@wordpressproyecto6:~$ sudo chmod -R 777 /var/www/html/
```

Esto lo haremos para evitar este error:

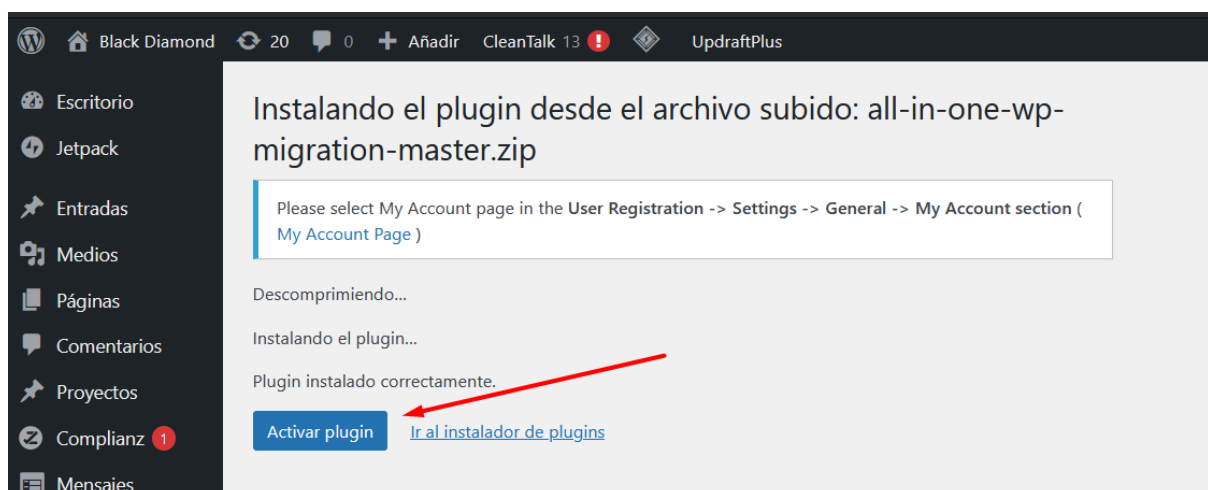
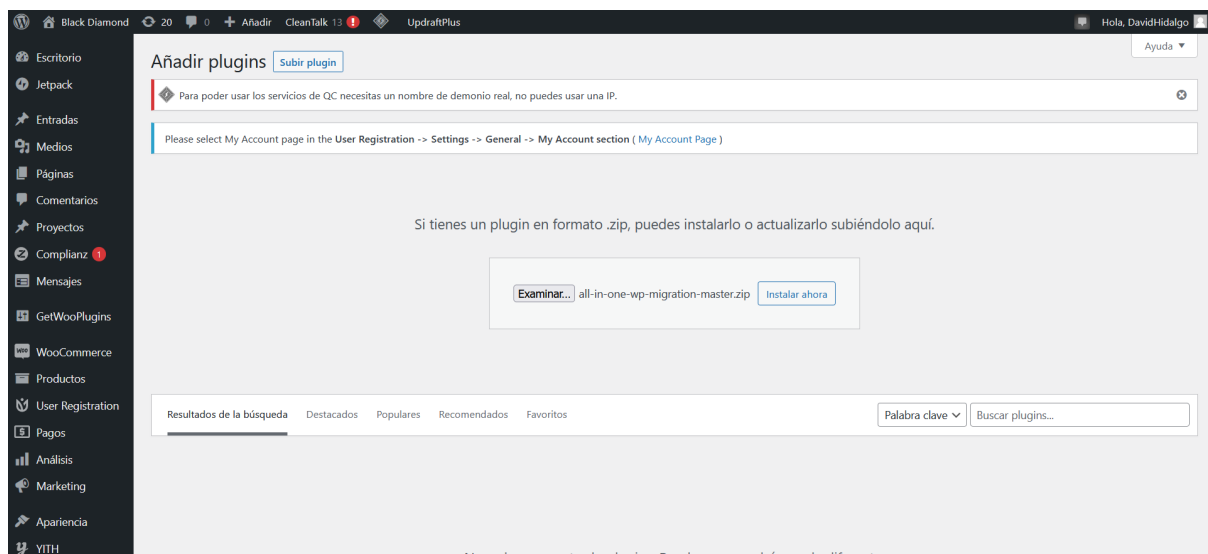
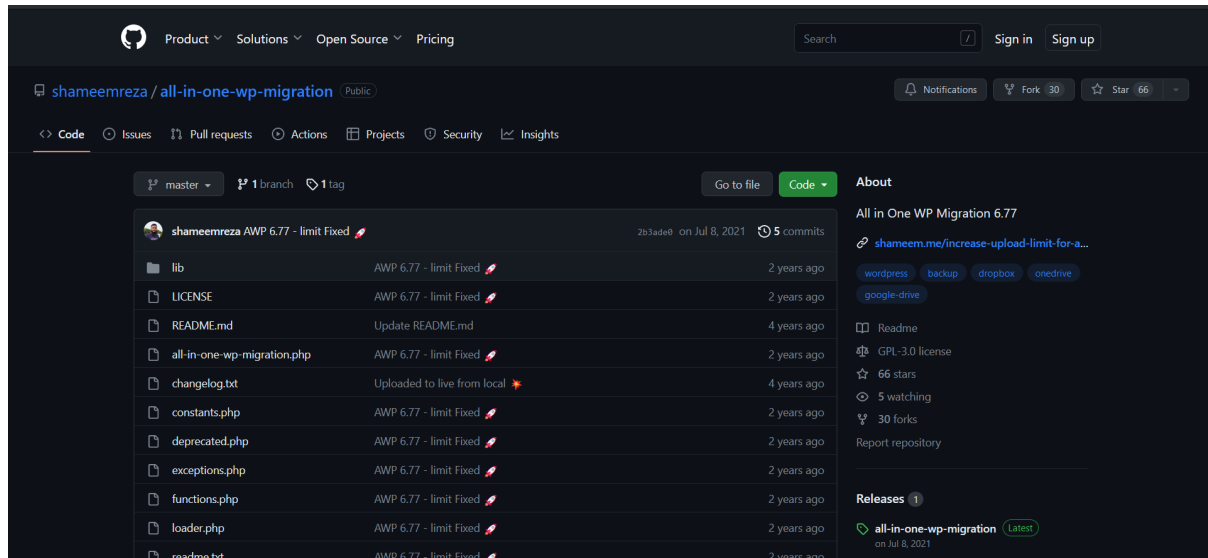
No ha sido posible crear el directorio /var/www/html/wp-content/upgrade

Ahora, con el usuario y contraseña definidos previamente, podemos iniciar sesión en WordPress.

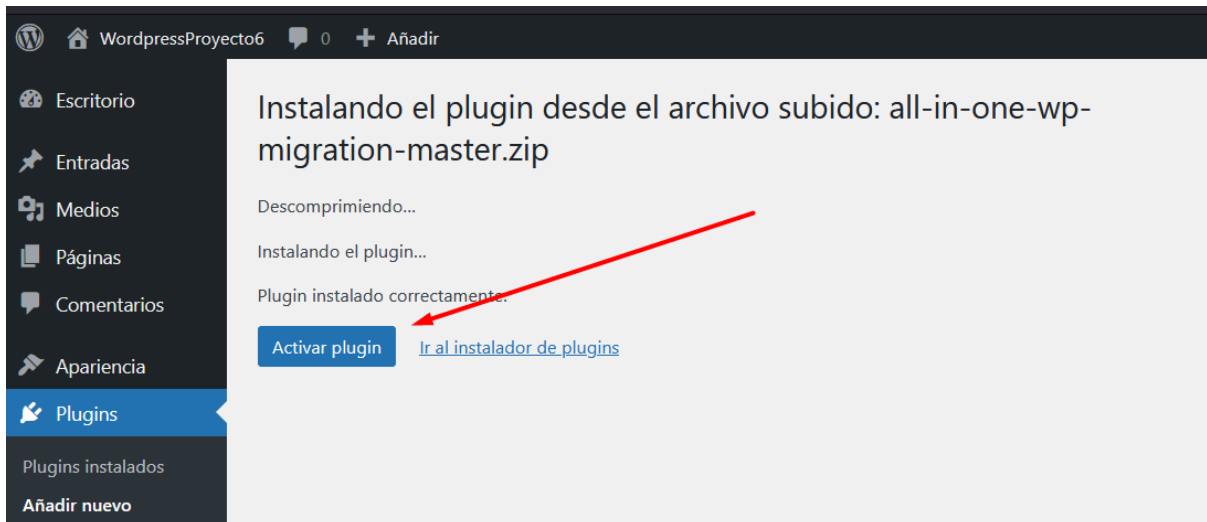
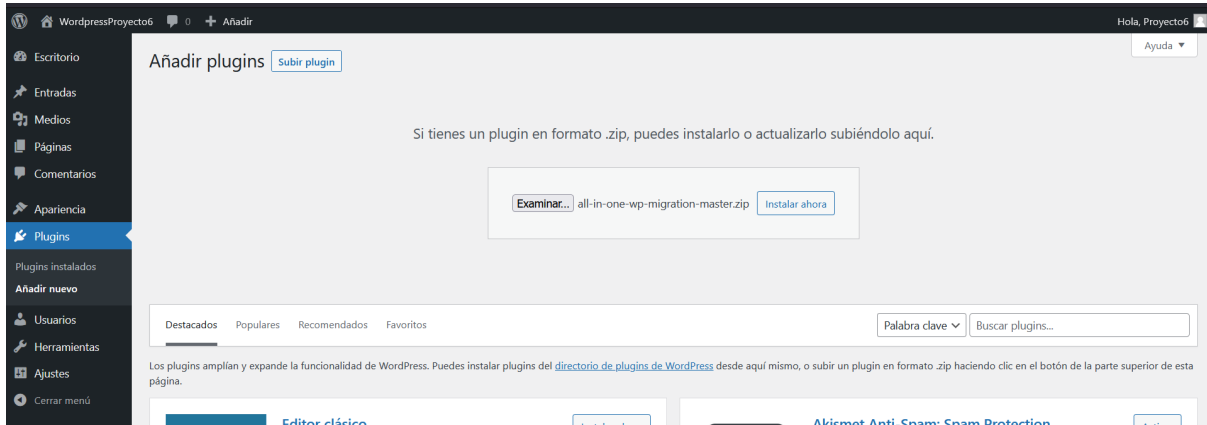


2- Guia de configuració de les diferents instal·lacions i serveis per a entregar-ho al client.

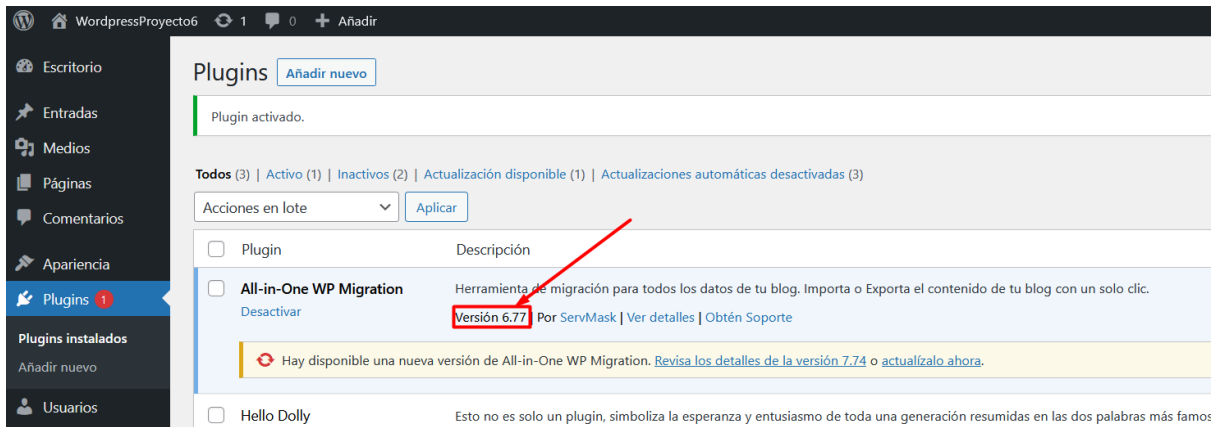
Instal·larem un plug-in para poder migrar la web, en este caso utilizarem el All-in-One Migration, [en la versión 6.77](#), para mayor tamaño de subida de archivos en la exportación.



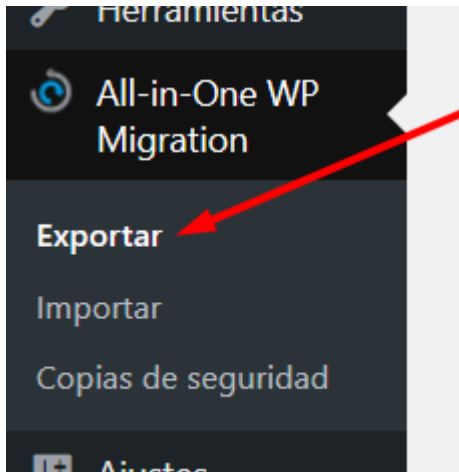
Haremos lo mismo en la máquina que tenemos la página web que queremos migrar.



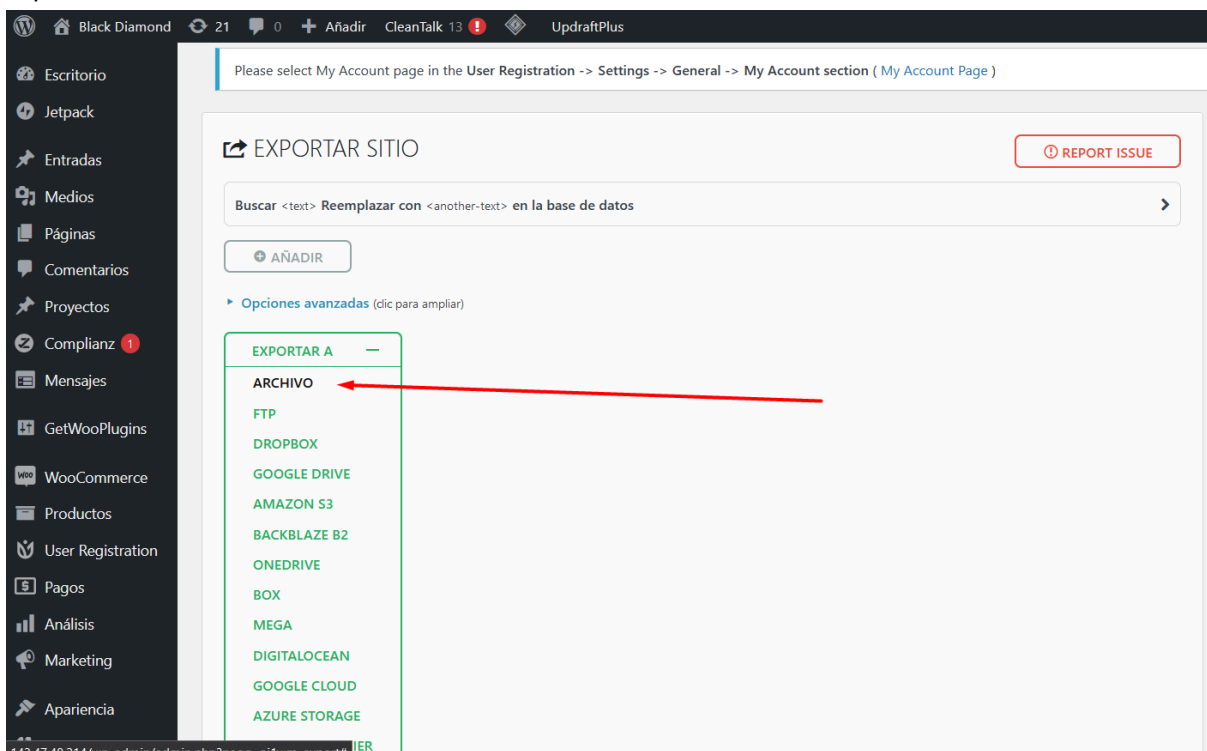
Y si vamos a ver la lista de plug-ins, veremos que tenemos la versión 6.77.



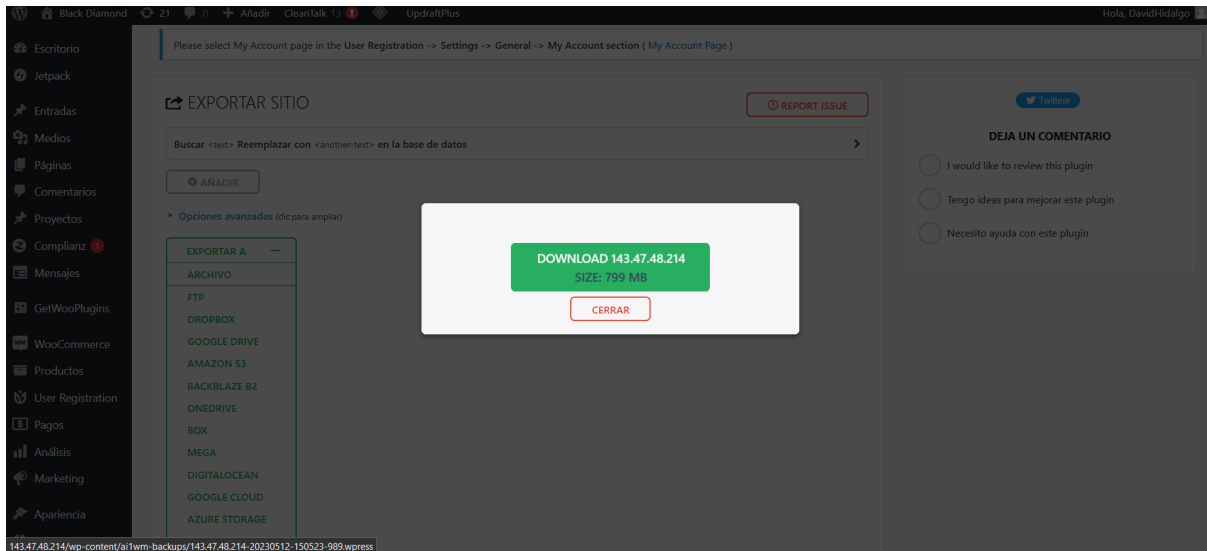
Una vez instalados los plug-ins en los dos WordPress, iremos a la página que queremos exportar y entraremos en el apartado del menú del "All-in-One Migration".



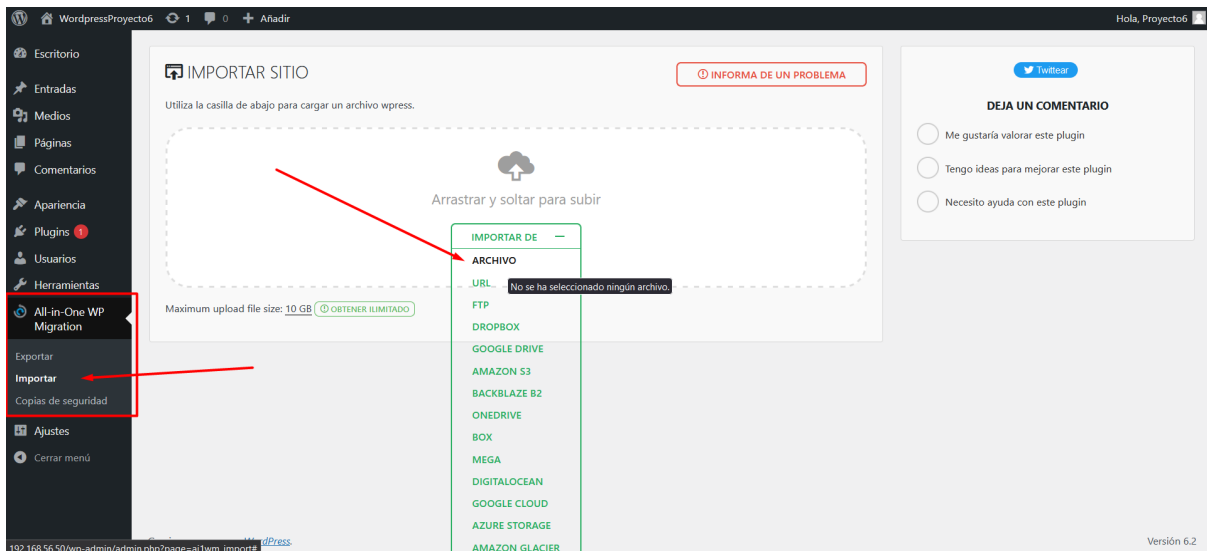
Exportamos nuestra web en un archivo.



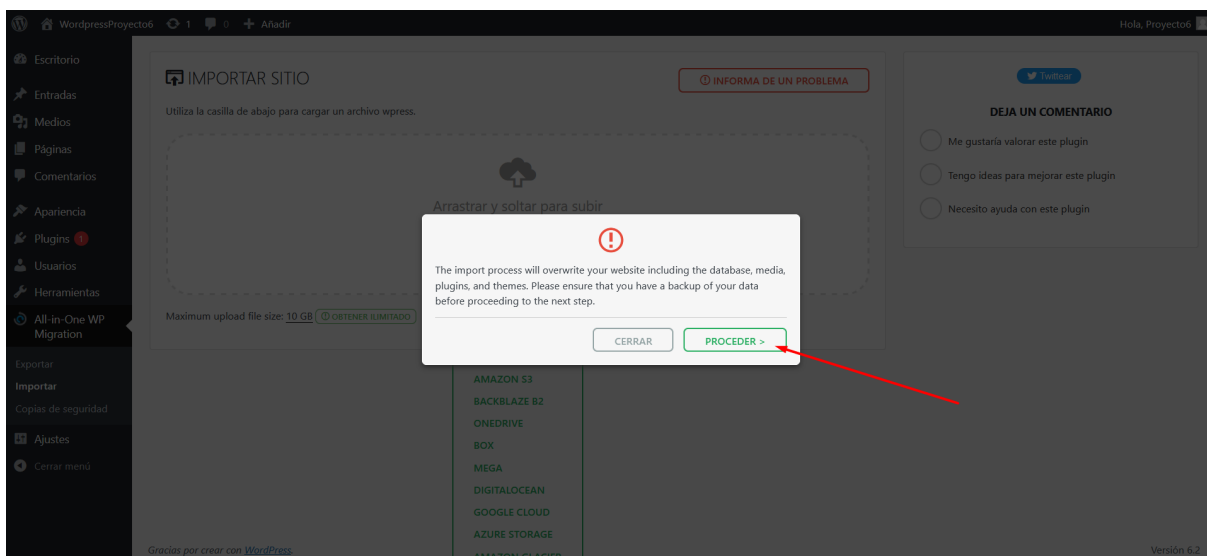
Nos generará el archivo que tendremos que guardar e importar en la otra web.



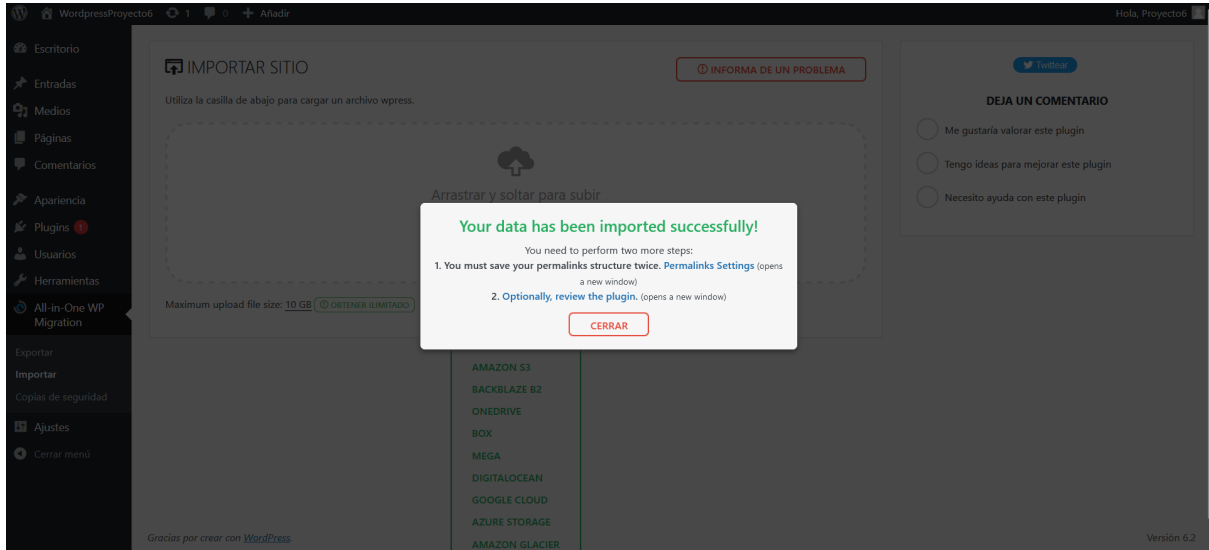
Ahora, dentro de la web que queremos importar el archivo, entraremos al apartado “Importar” dentro del menú del plug-in y seleccionamos la opción de importar desde un archivo.



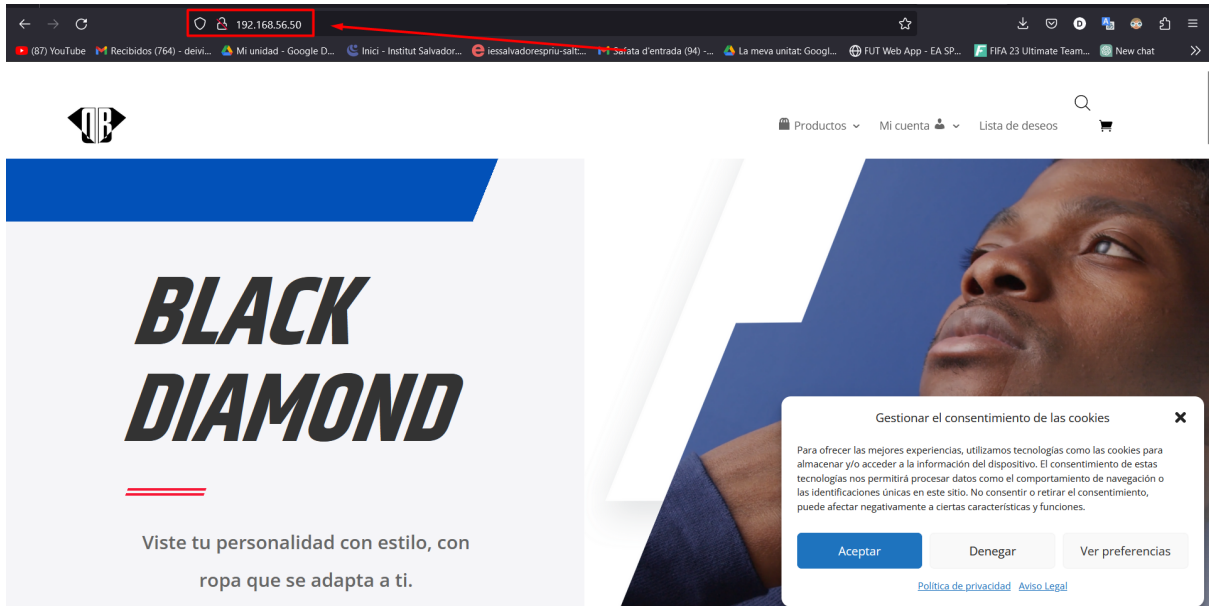
Cuando se acabe de importar la página, nos saldrá un aviso de que se sobrescribirá la web que tenemos.



Cuando le demos clic, empezará la restauración. Una vez acabado, saldrá este mensaje:

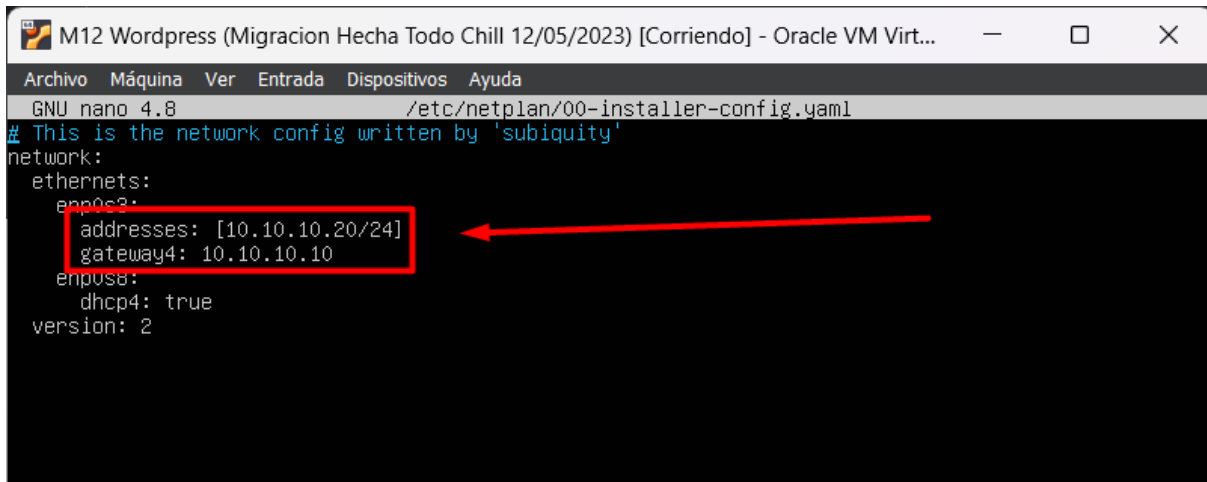


Como podemos ver ahora, si accedemos a la IP de la interfaz Host-Only, veremos la Web que teníamos en el otro proyecto.



3- Configuració del servei dins d'una infraestructura segura.

Configuramos la red en el netplan.



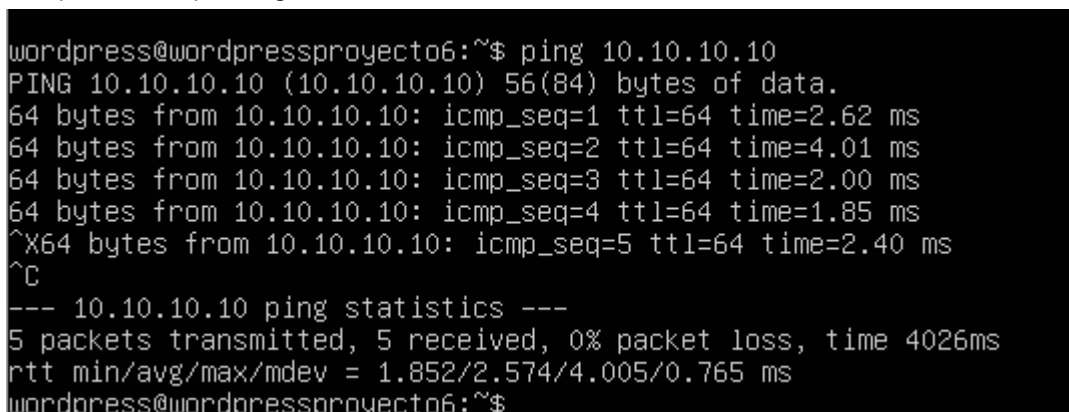
```

M12 Wordpress (Migracion Hecha Todo Chill 12/05/2023) [Corriendo] - Oracle VM Virt...
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 4.8 /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0c3:
      addresses: [10.10.10.20/24]
      gateway4: 10.10.10.10
    enp0s8:
      dhcp4: true
  version: 2
  
```

Aplicamos el netplan.

```
wordpress@wordpressproyecto6:~$ sudo netplan apply
```

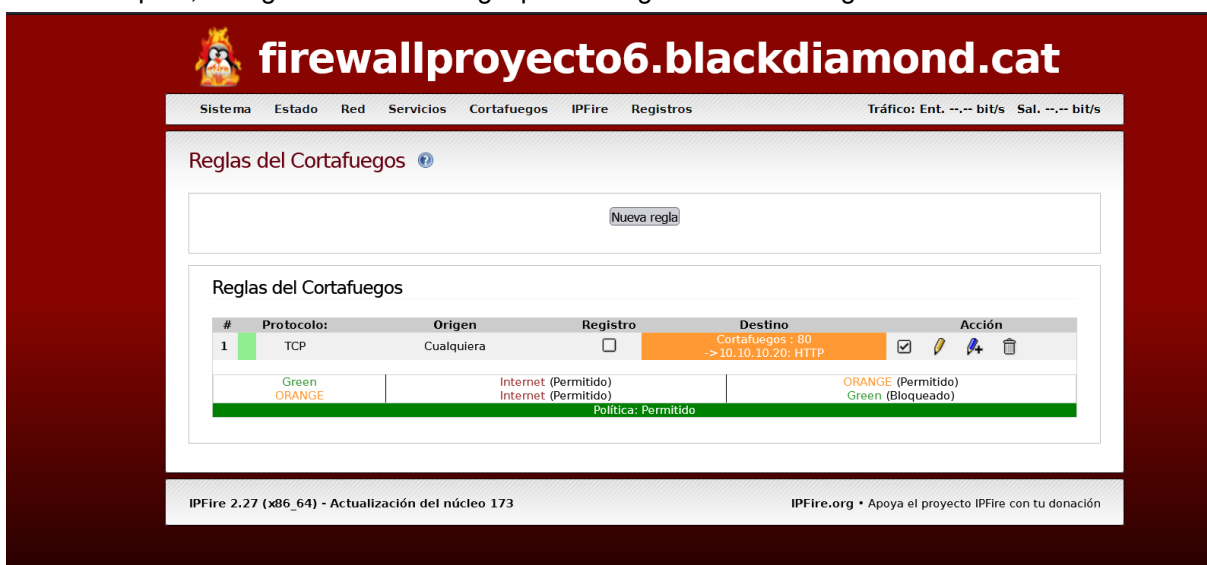
Comprobamos que tengamos conexión con el firewall.



```

wordpress@wordpressproyecto6:~$ ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=64 time=2.62 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=64 time=4.01 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=64 time=2.00 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=64 time=1.85 ms
^X64 bytes from 10.10.10.10: icmp_seq=5 ttl=64 time=2.40 ms
^C
--- 10.10.10.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4026ms
rtt min/avg/max/mdev = 1.852/2.574/4.005/0.765 ms
wordpress@wordpressproyecto6:~$
  
```

Dentro del ipfire, configuraremos esta regla para configurar la red Orange.



firewallproyecto6.blackdiamond.cat

Sistema Estado Red Servicios Cortafuegos IPFire Registros Tráfico: Ent. -- bit/s Sal. -- bit/s

Reglas del Cortafuegos ?

Nueva regla

Reglas del Cortafuegos

#	Protocolo	Origen	Registro	Destino	Acción
1	TCP	Cualquiera	<input type="checkbox"/>	Cortafuegos : 80 ->10.10.10.20: HTTP	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	Green	Internet (Permitido)		ORANGE (Permitido)	
	ORANGE	Internet (Permitido)		Green (Bloqueado)	
Política: Permitido					

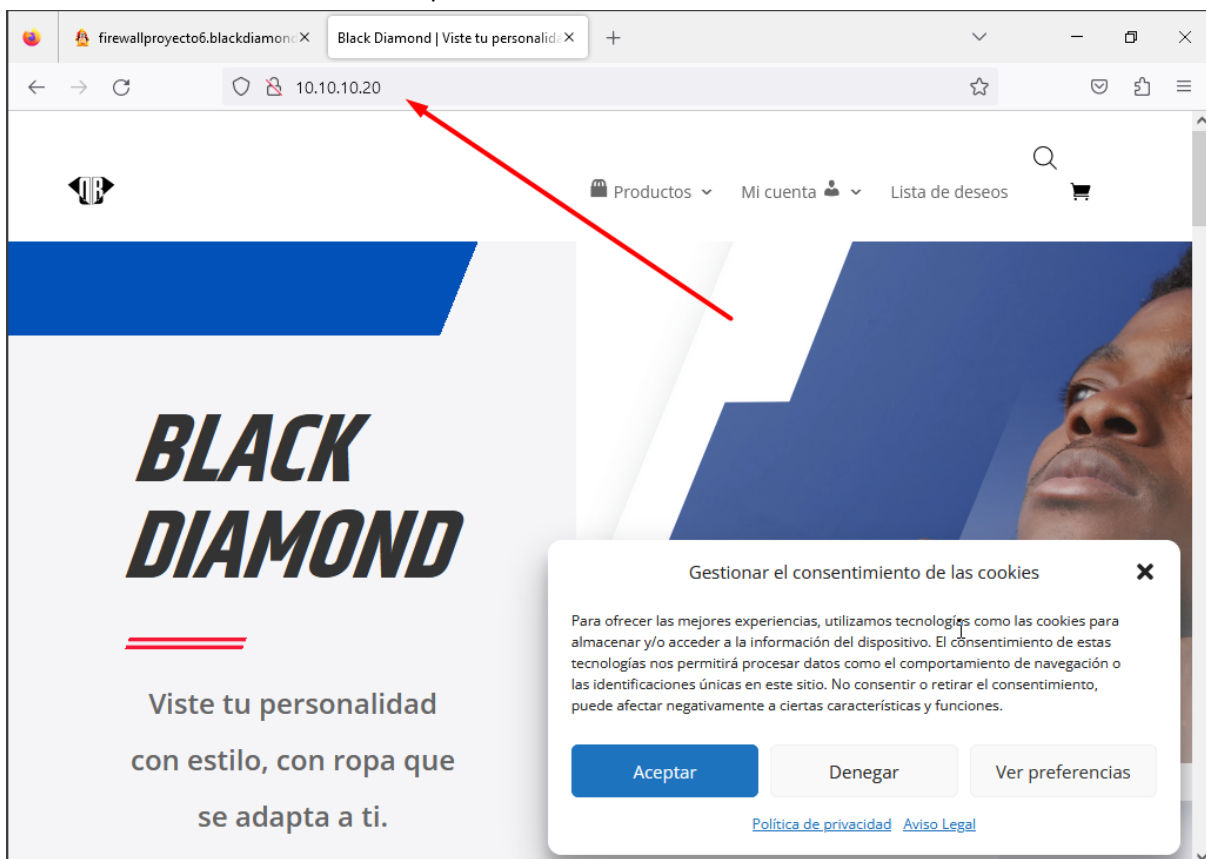
IPFire 2.27 (x86_64) - Actualización del núcleo 173 IPFire.org • Apoya el proyecto IPFire con tu donación

Si probamos de entrar a la web desde una máquina que esté dentro de la red green, podemos entrar a la página web. Configuramos el archivo DNS, para que redireccione la URL www.blackdiamond.cat a la IP 10.10.10.20, que es nuestro servidor web.

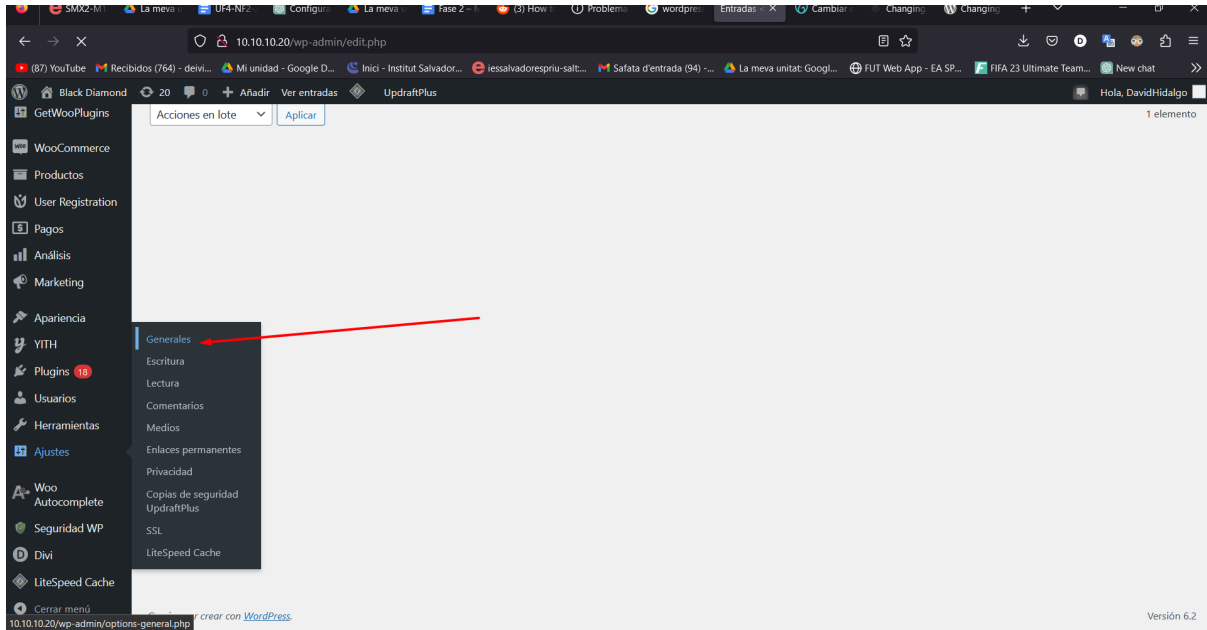
```
Ubuntu Server DNS (17-04-23) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU nano 4.8 /etc/bind/db.blackdiamond

; BIND data file for local loopback interface
$TTL 604800
@ IN SOA blackdiamond.cat. root.blackdiamond.cat. (
        2 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS blackdiamond.cat.
@ IN A 192.168.1.3
@ IN AAAA ::1
dnsproyecte5 IN IN A 192.168.1.3
m4usdh IN IN A 192.168.1.4
www IN IN A 10.10.10.20
```

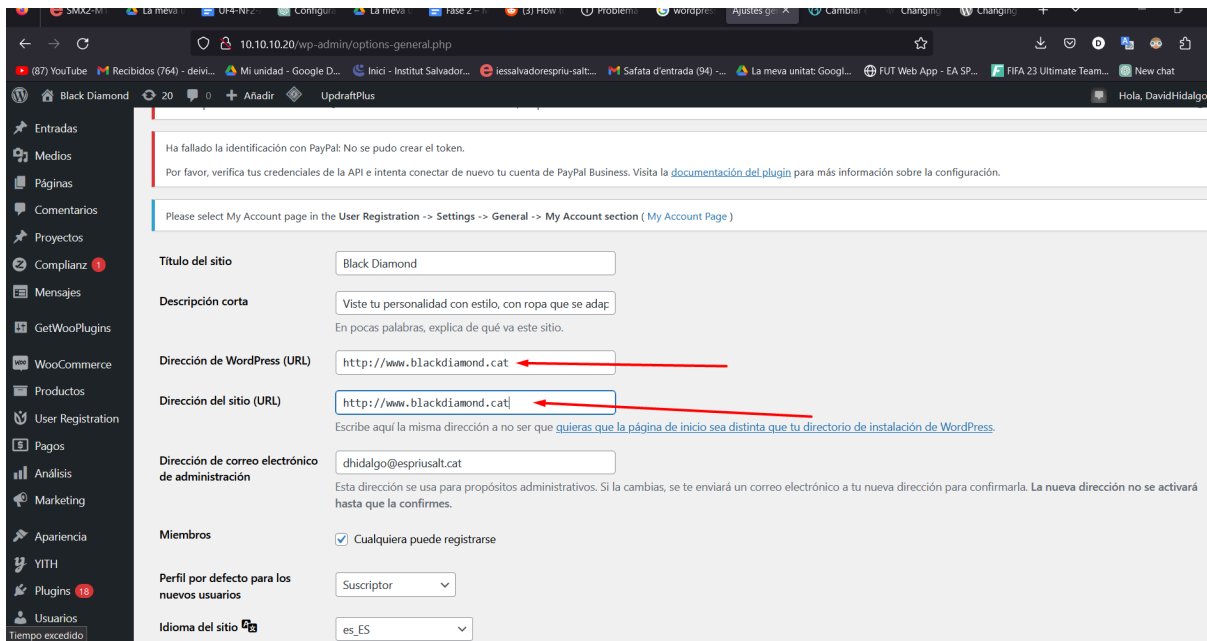
Entraremos a la web desde la URL, pero nos continuará redireccionando a la IP.



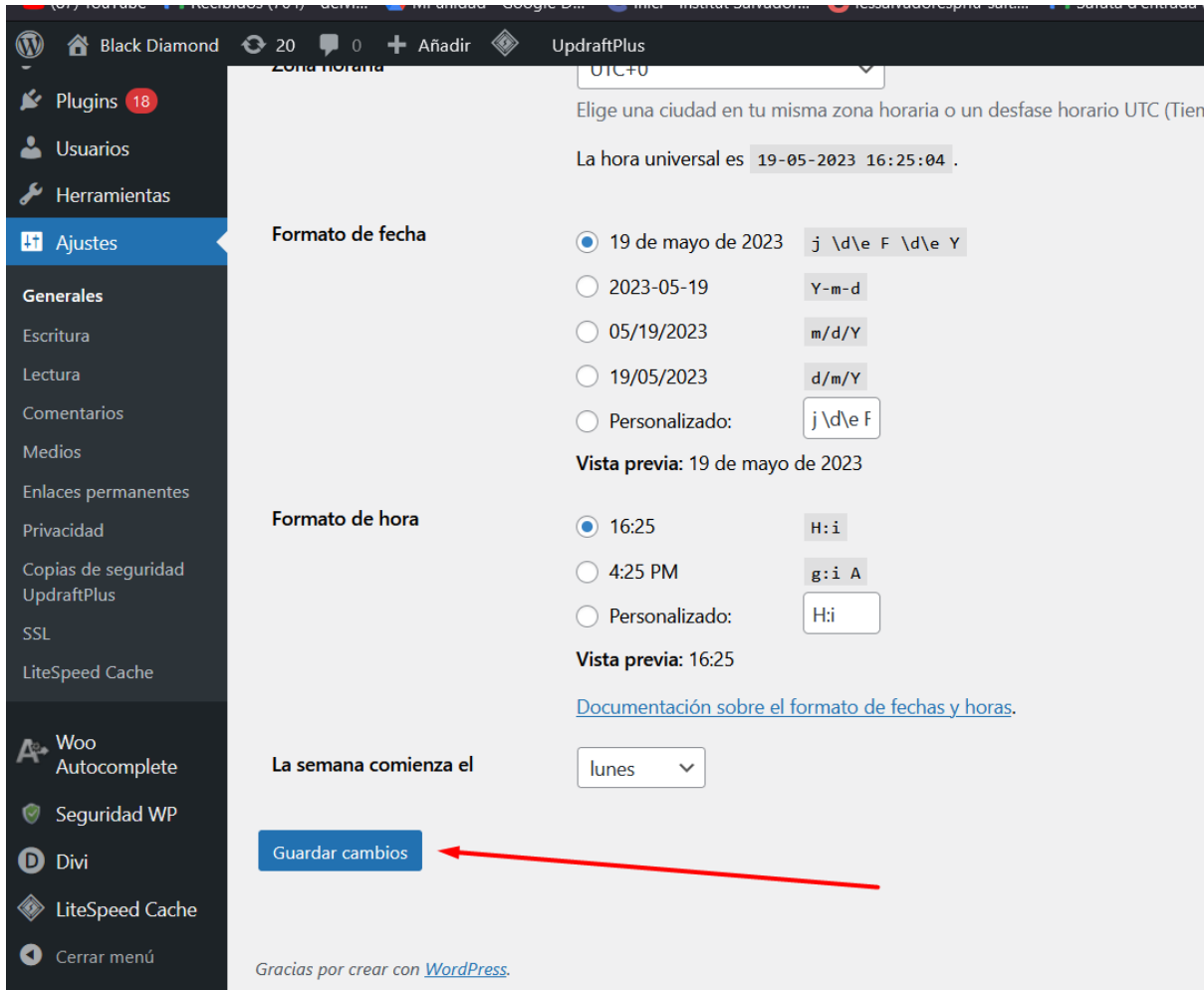
Para cambiar la URL de la web, debemos ir a Ajustes>Generales.



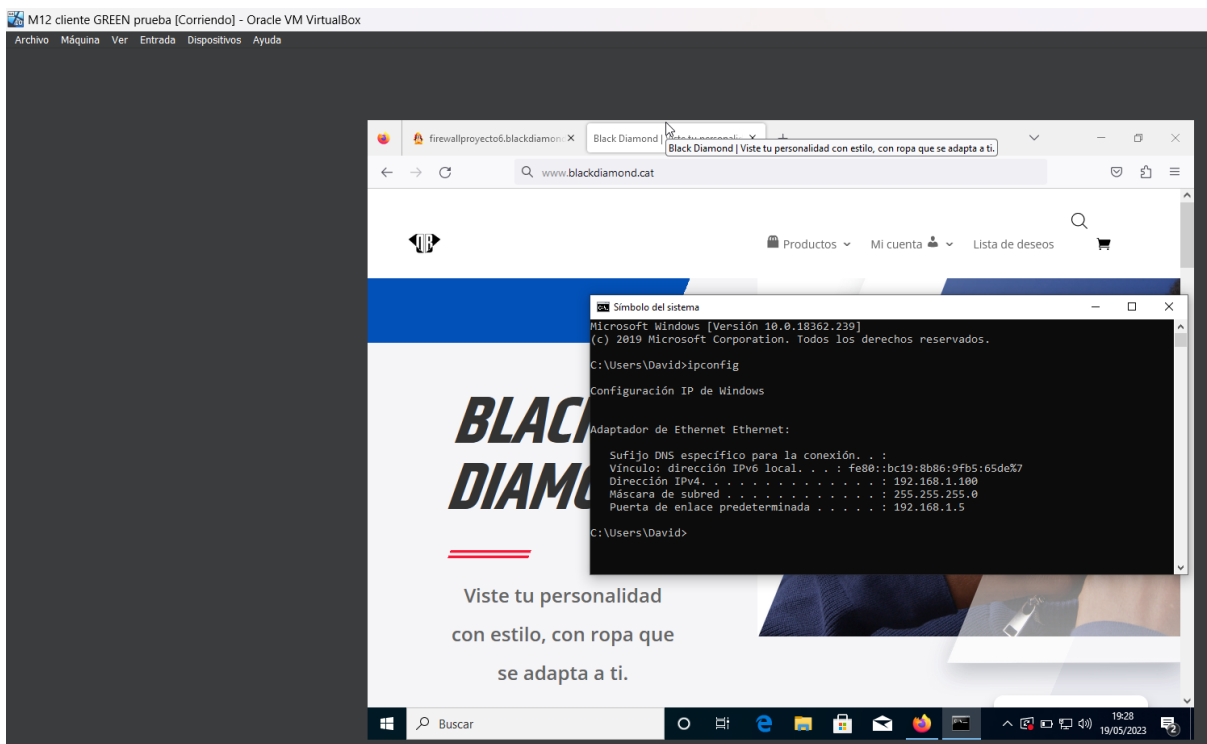
Y en los ajustes de dirección de WordPress y del sitio la cambiaremos por la URL que queramos.



Guardamos los cambios que hemos hecho.



Y ahora podemos acceder desde la URL desde la GREEN.



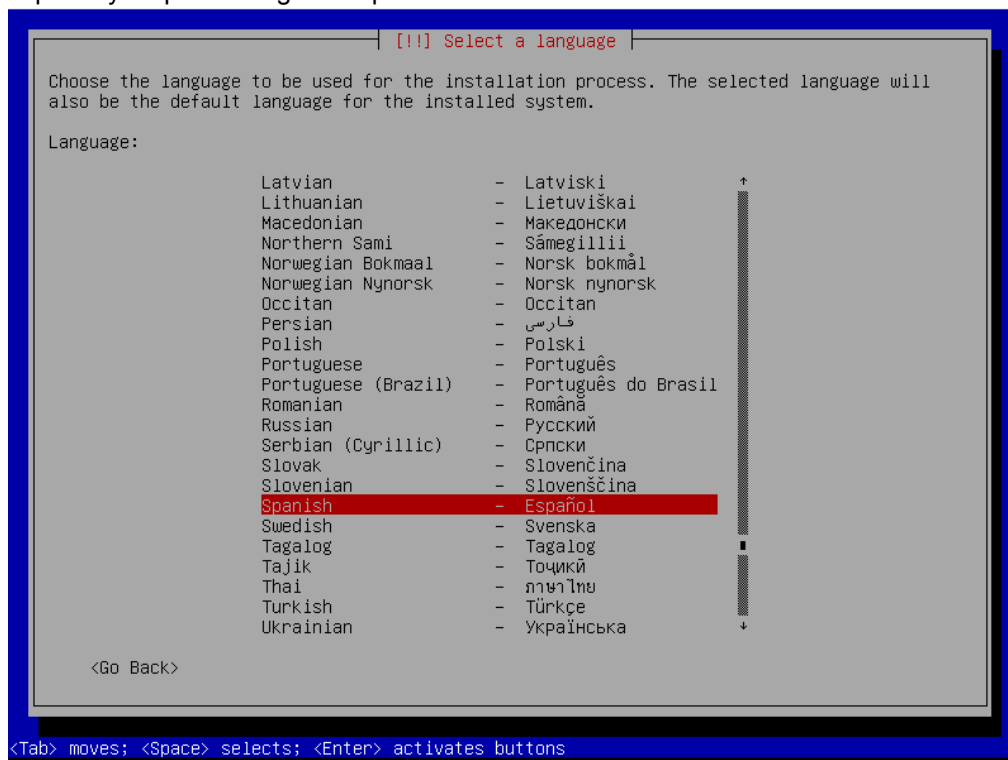
Fase 3 – Gestió de documents (6h)

1- Instal·lació d'un sistema d'emmagatzemament en xarxa.

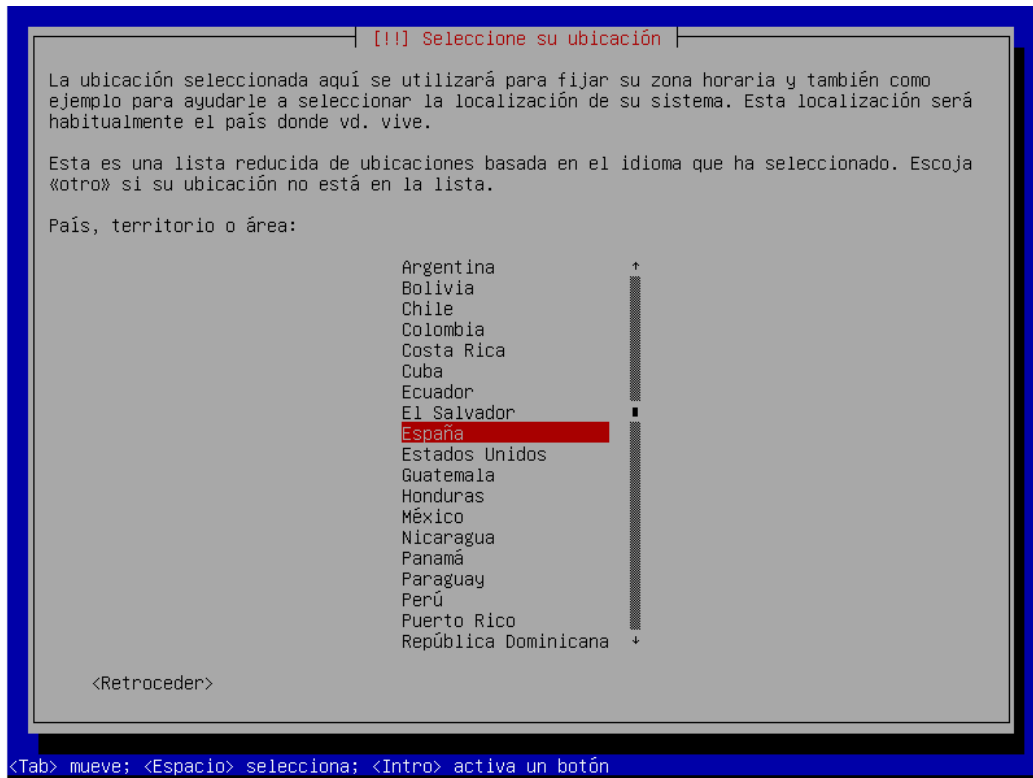
En el caso del NAS, se decidió utilizar una distribución de Linux para NAS, la cual te trae muchas facilidades para hacer RAID, compartir carpetas... En este caso se utilizó [Open Media Vault](#) entre otras por su bajo consumo de recursos. Otra de las opciones era [QNAP](#), en ambos casos se incluye una interfaz web con SO a la que se podrá entrar y administrar todo lo relacionado con el NAS. En este caso se decidió hacer un RAID 10 porque en un NAS es mejor para empresas porque combina velocidad y protección de datos. Ofrece un rendimiento más rápido al escribir y leer datos, y tiene alta tolerancia a fallos. Además, permite más capacidad de almacenamiento y es fácil de ampliar.

Primero se creará los VDI de los discos que se van a utilizar de almacenamiento para el NAS, en este caso se utilizan 6 discos de 10GB, en un principio se intentó hacer con 6 discos de 1TB pero la creación del RAID 10 tardaba demasiado y se decidió cambiar a 6 discos de 10GB haciendo así que el NAS tenga un almacenamiento final de 30GB.

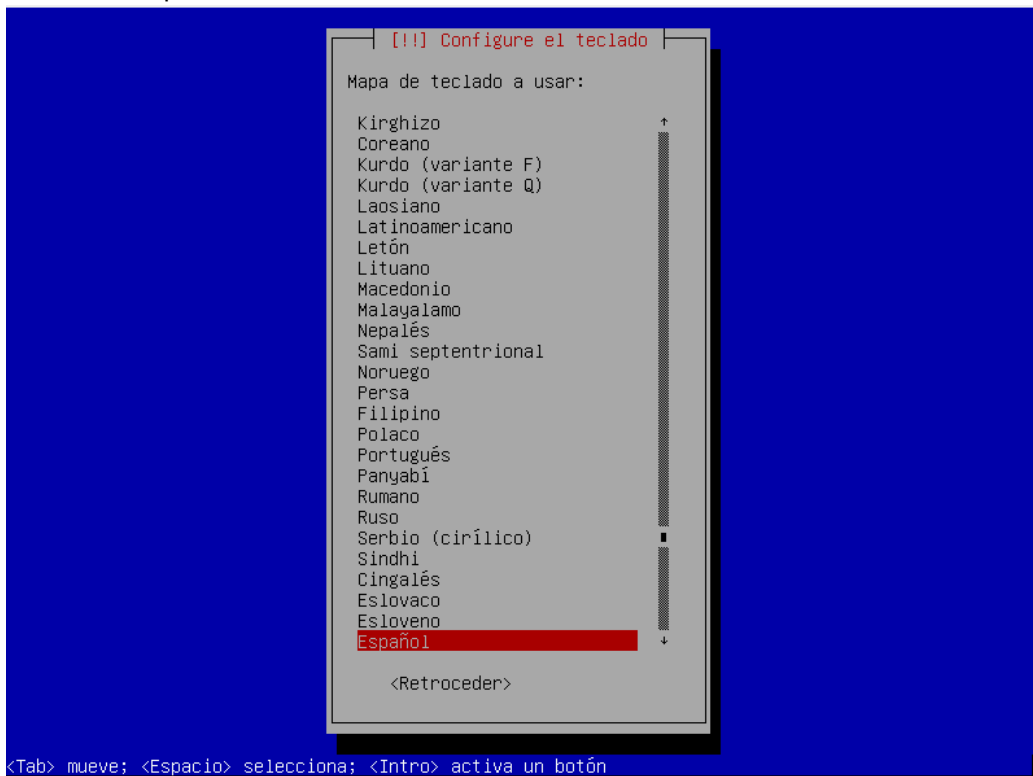
En primer lugar al realizar la instalación se deberá configurar el idioma del NAS, se selecciona Español y se pasa al siguiente paso.



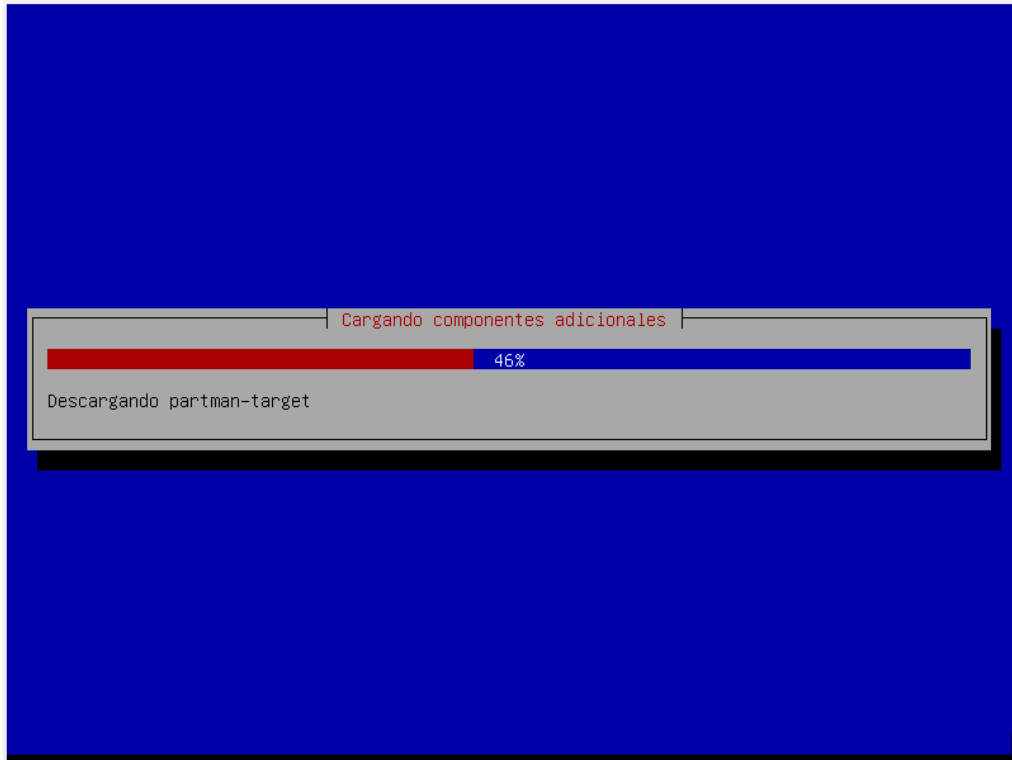
Acto seguido se deberá seleccionar la ubicación para la zona horaria del NAS, en este caso España.



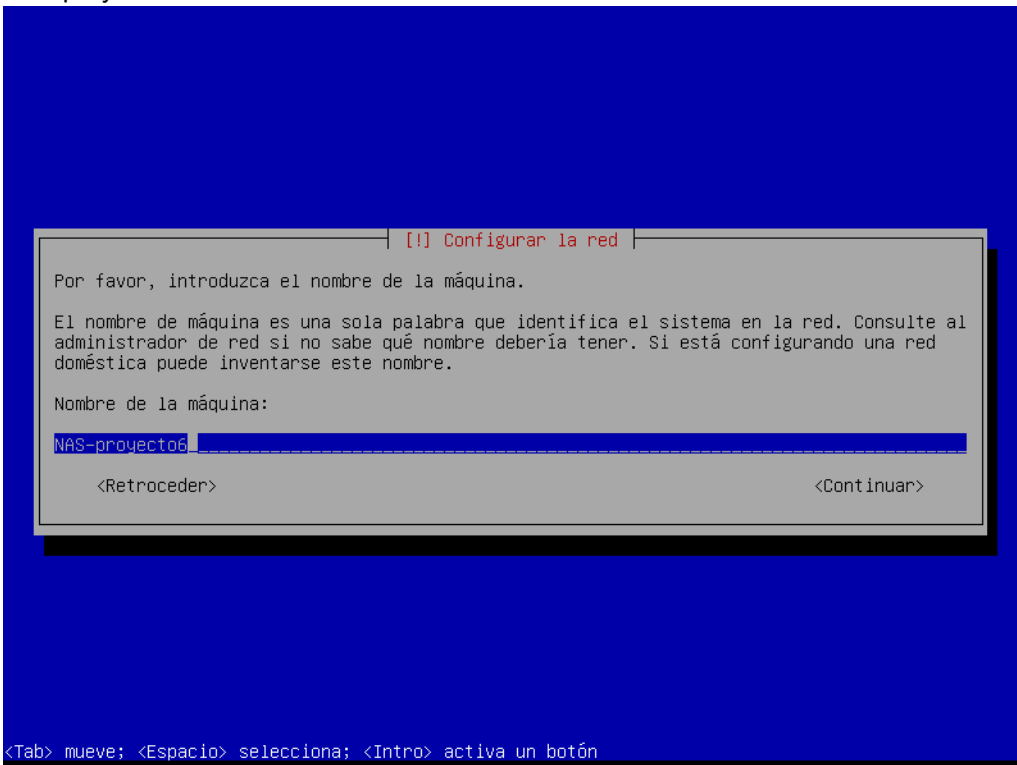
Para continuar se deberá seleccionar la distribución de teclado, en este caso se seleccionará el teclado en Español.



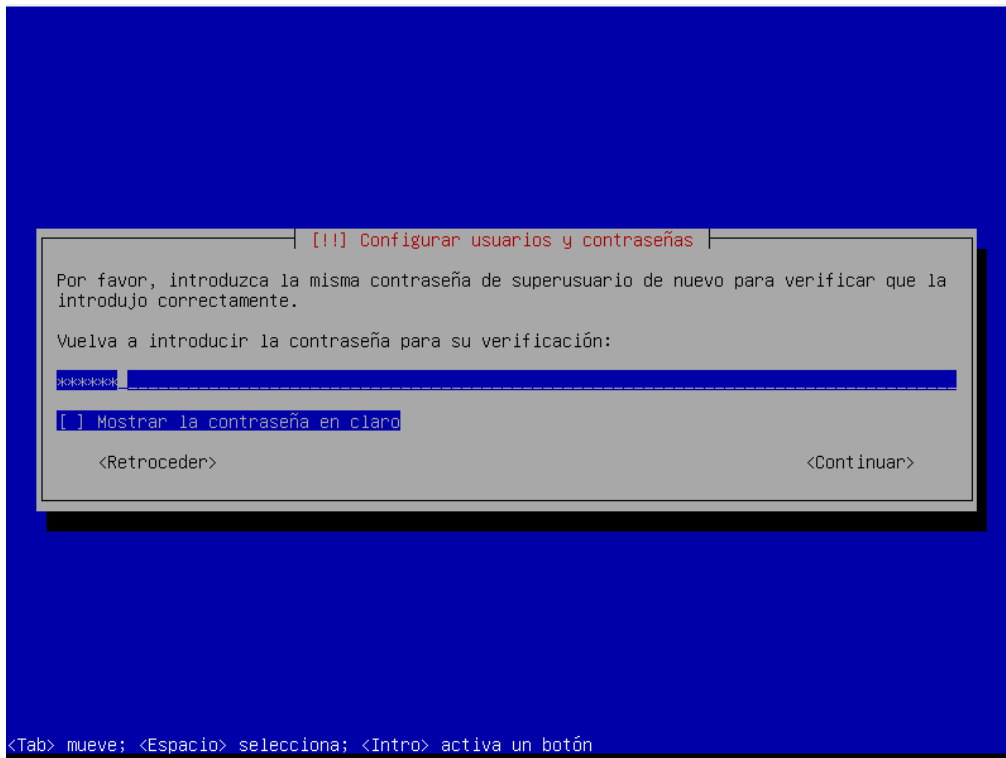
Después de seleccionar el mapa de teclado a utilizar se iniciará la instalación del SO.



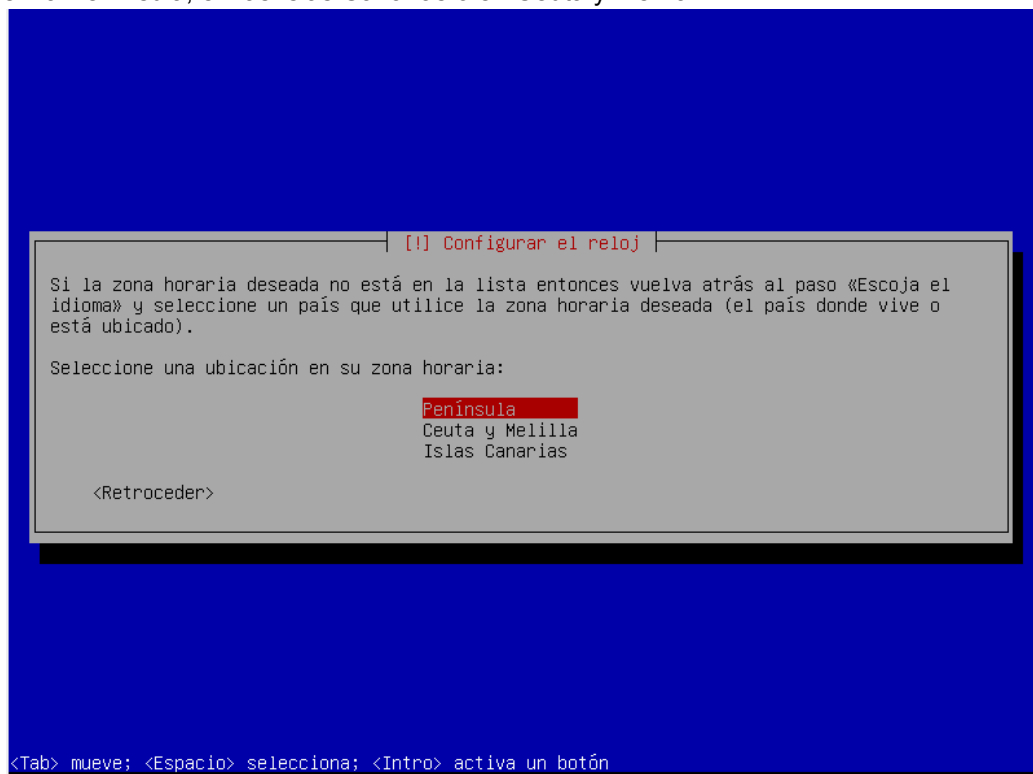
Al finalizar la instalación se solicitará el hostname de la máquina, en este caso el hostname será NAS-proyecto6.



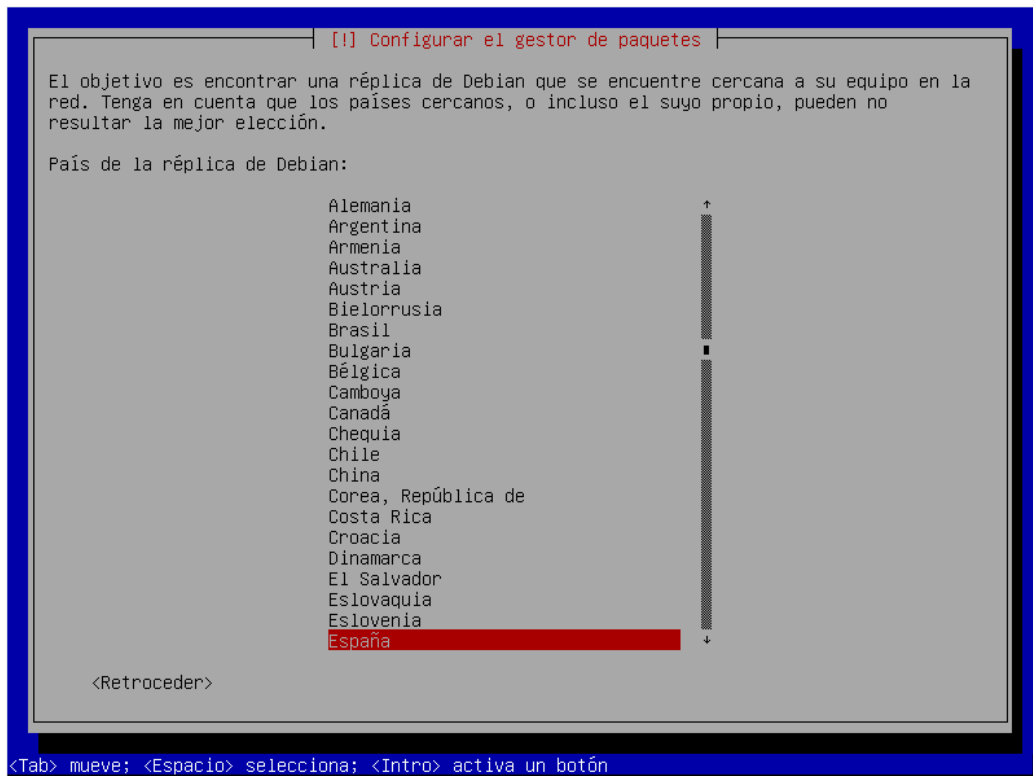
Una vez se tenga el hostname de la máquina se nos pedirá una contraseña de acceso para el superusuario y acto seguido se deberá confirmar, en este caso se utilizará como contraseña 123456.



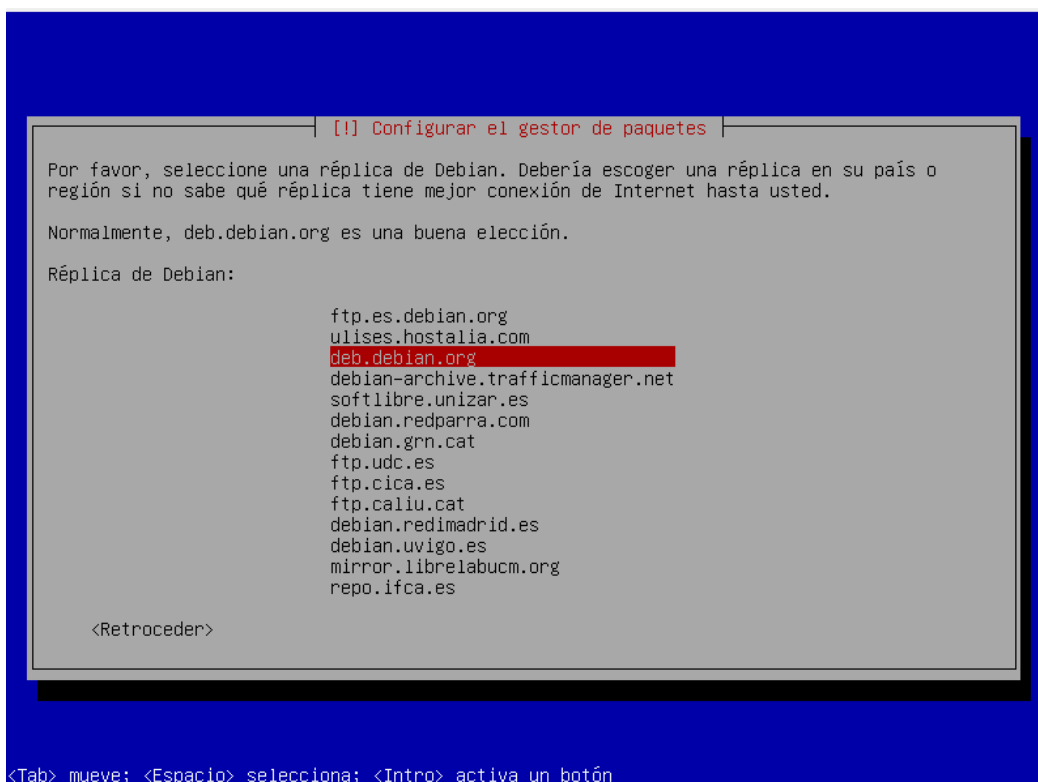
En este caso, como España consta con varias zonas horarias, se deberá seleccionar si te encuentras en la Península, en las Islas Canarias o en Ceuta y Melilla.



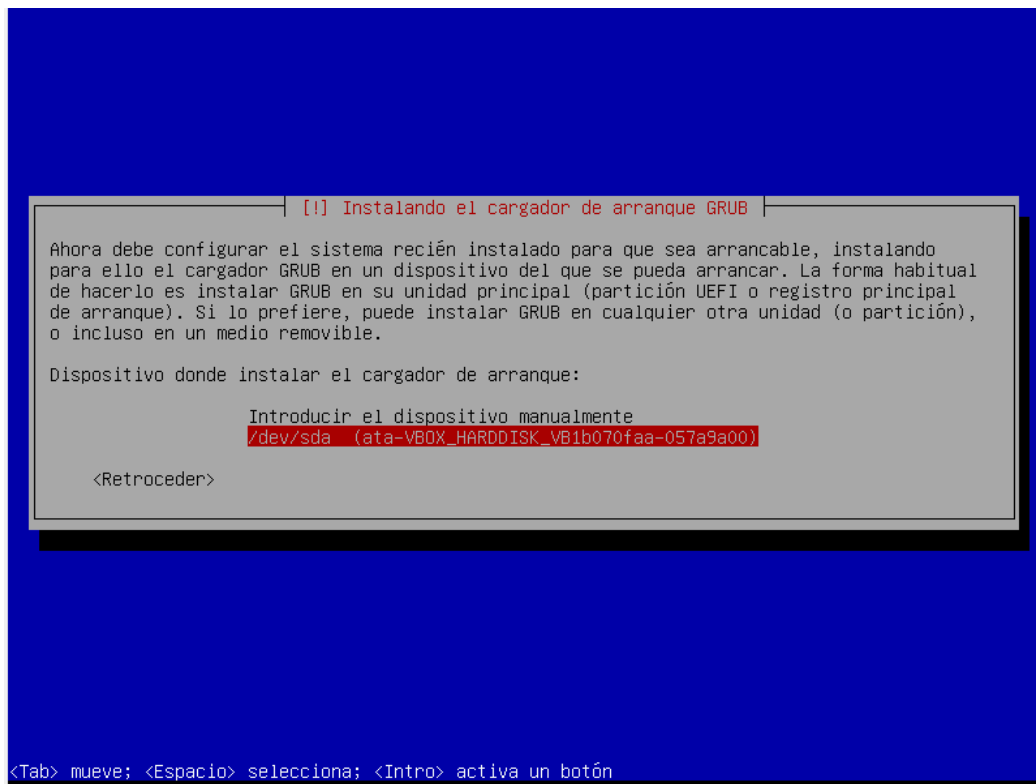
Seguidamente, tenemos que seleccionar la configuración del gestor de paquetes, seleccionando la réplica del país correspondiente, en este caso escogemos "España".



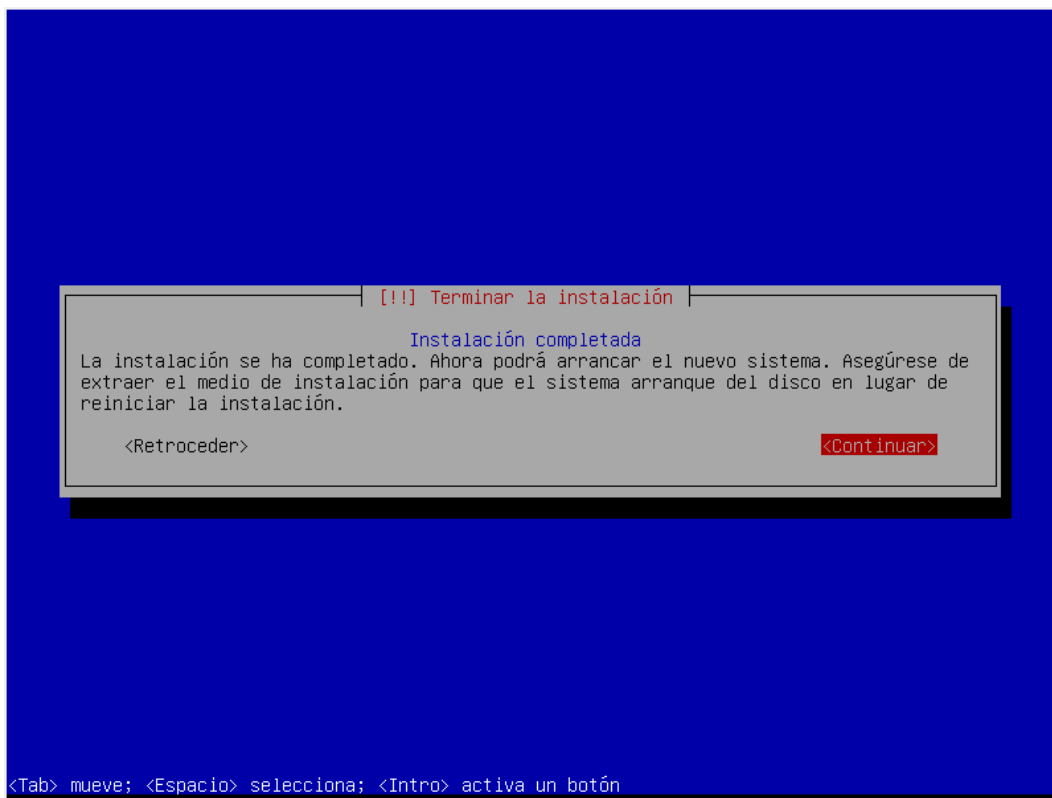
Seguidamente, tenemos que escoger la réplica de Debian, es esta parte seleccionamos el que esta seleccionado por defecto el “deb.debian.org”



Y finalmente seleccionamos el disco donde se va a instalar el cargador de arranque para nuestra máquina.



Le damos a “continuar” para que se termine la instalación.

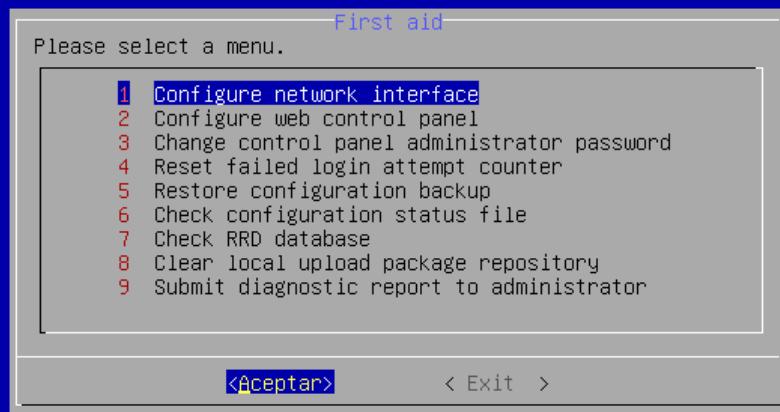


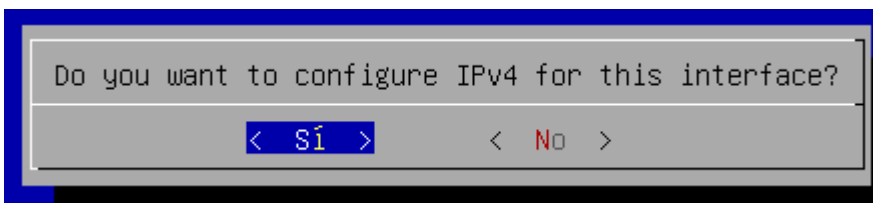
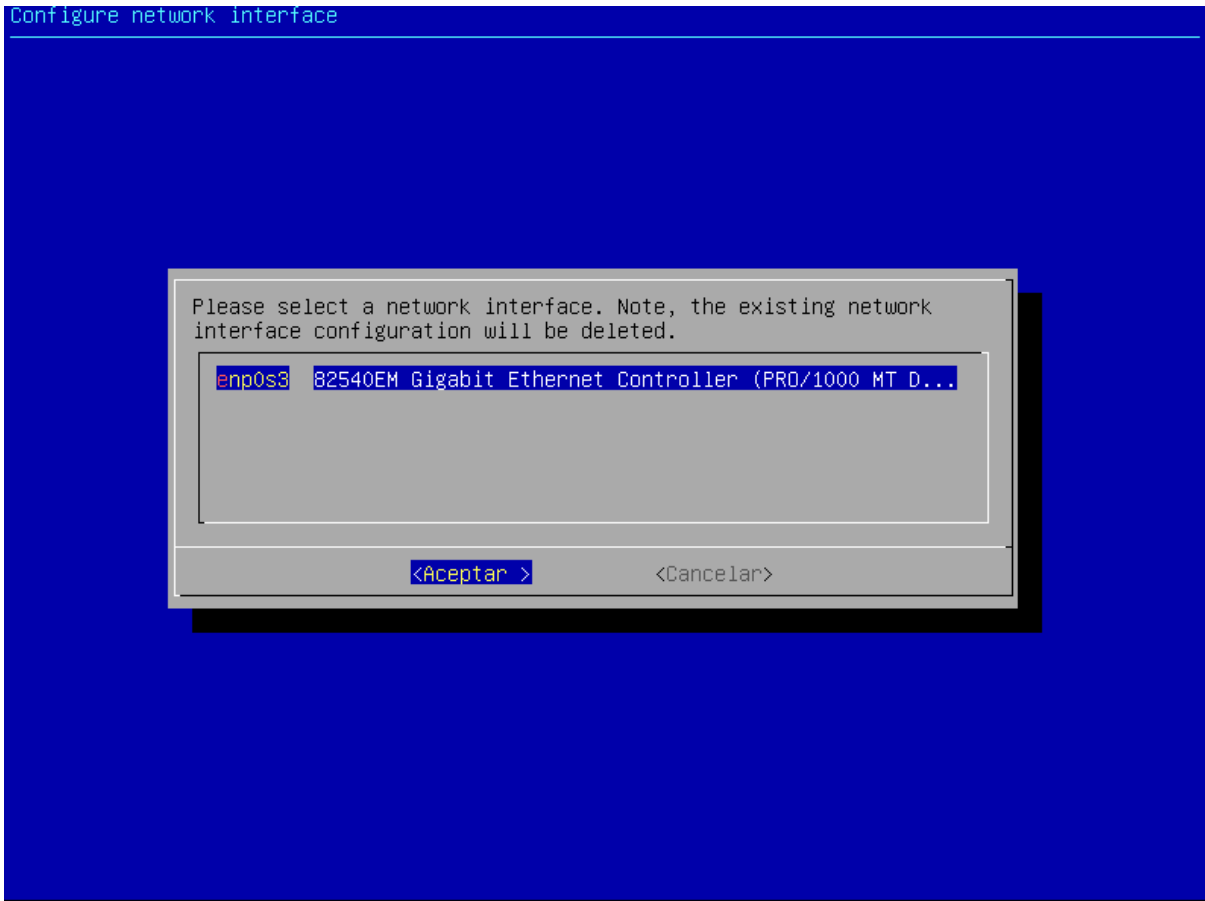
Una vez completada la instalación del SO se deberá utilizar el comando `omv-firstaid` para configurar todo el SO del NAS.

```
root@NAS-proyecto6:~# omv-firstaid_
```

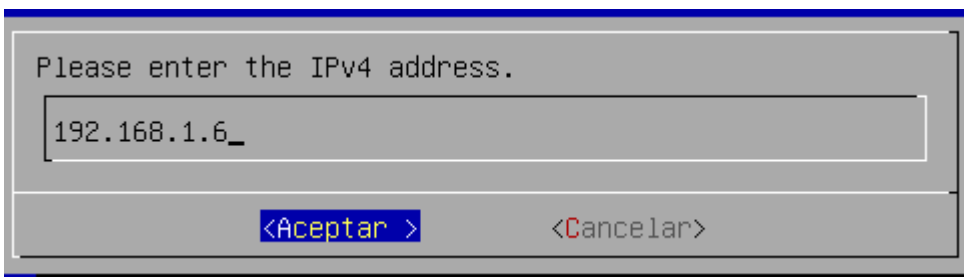
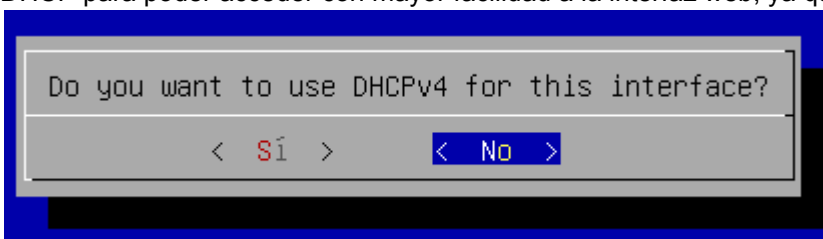
Como primera opción se deberá configurar la red, para esto escogemos la opción “Configure network interface”, y le asignamos la ip a dispositivo, en este caso al adaptador de red del NAS se le asignará una IP 192.168.1.6/24.

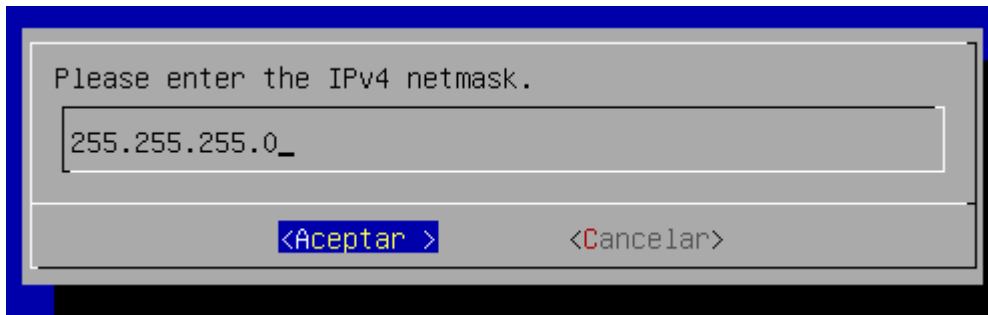
```
openmediavault - Copyright (C) 2009-2022 by Volker Theile. All rights reserved.
```





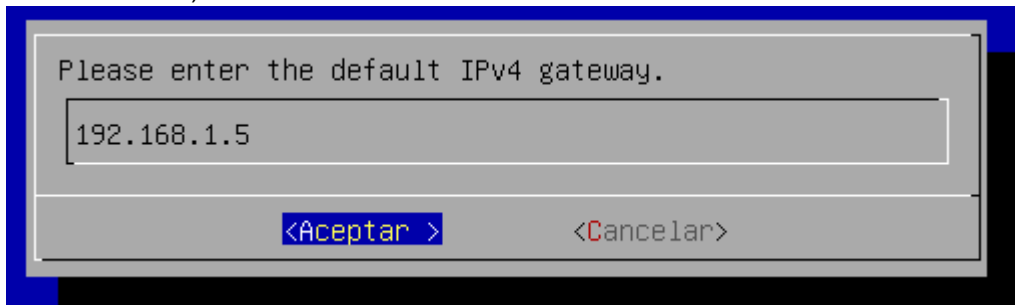
Aquí se preguntará si se desea utilizar DHCP para la máquina. En este caso se decidió no utilizar DHCP para poder acceder con mayor facilidad a la interfaz web, ya que contará con una IP estática.



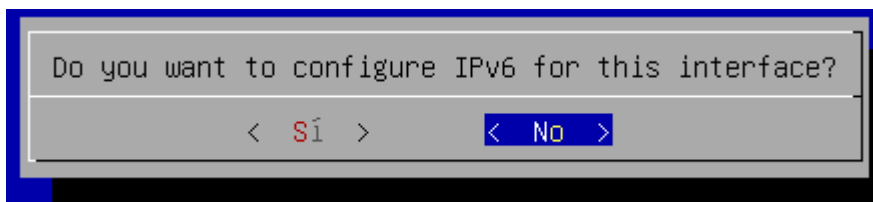


```
Please enter the IPv4 netmask.
255.255.255.0_
<Aceptar > <Cancelar >
```

Cuando se solicite el GTW se deberá poner la IP de nuestro GTW del Firewall IPFire (La que tiene salida a internet). Esta IP será la 192.168.1.5

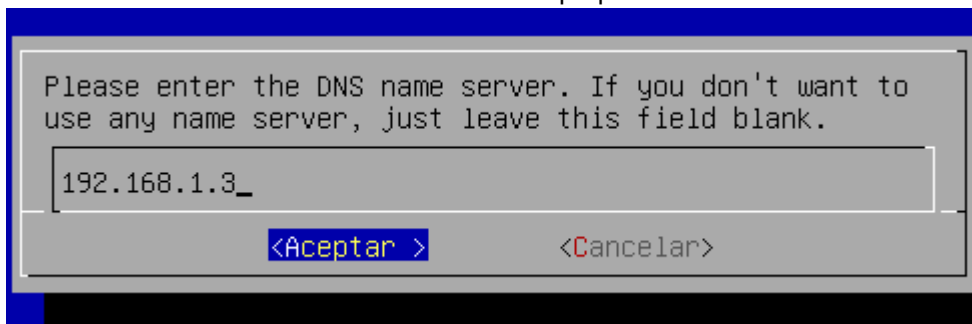


```
Please enter the default IPv4 gateway.
192.168.1.5
<Aceptar > <Cancelar >
```



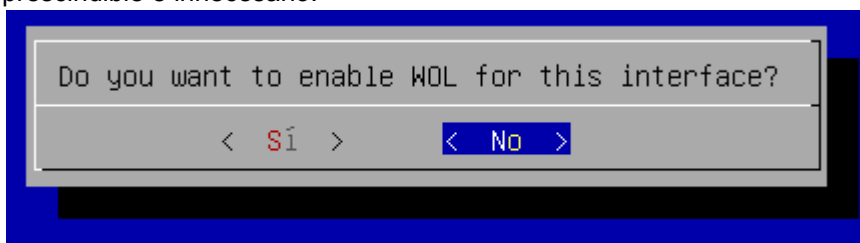
```
Do you want to configure IPv6 for this interface?
< Sí > < No >
```

El servidor DNS a utilizar será el servidor DNS propio de la red con IP 192.168.1.3



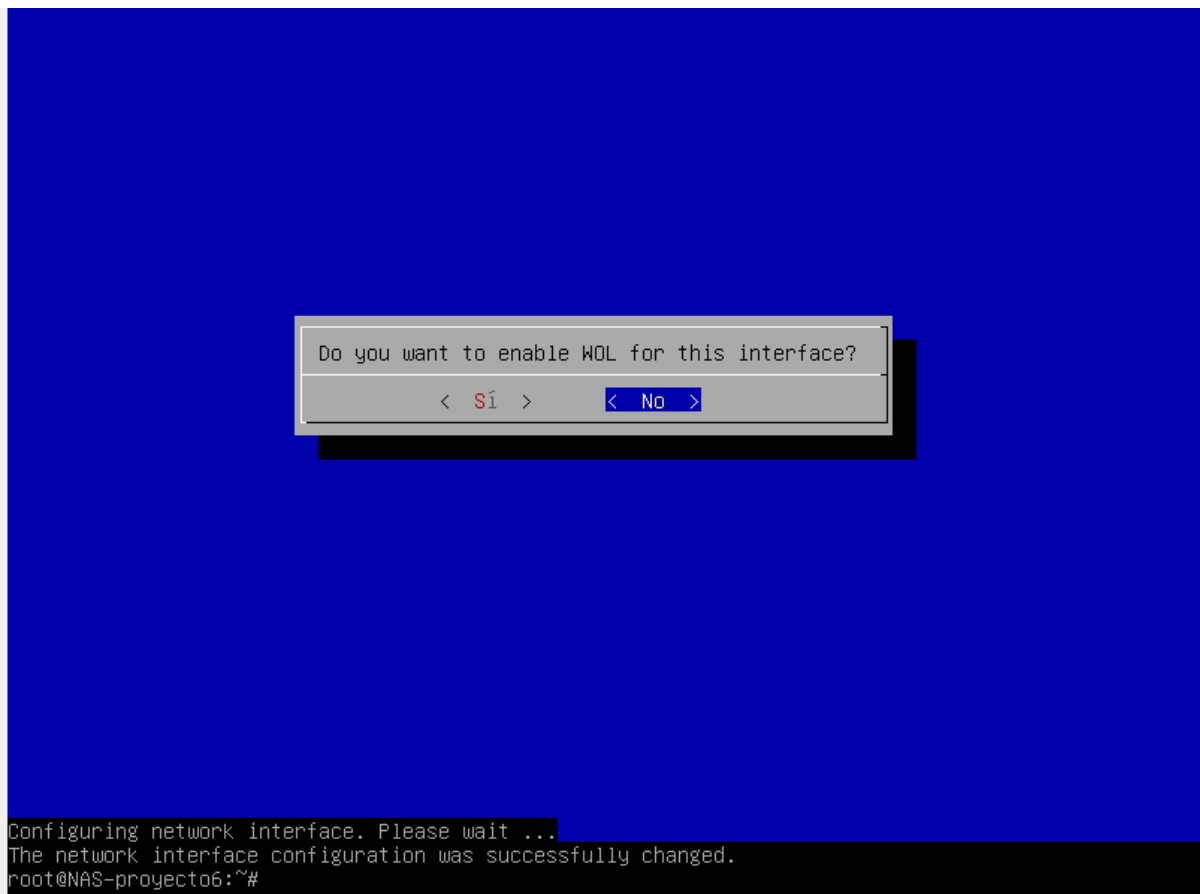
```
Please enter the DNS name server. If you don't want to
use any name server, just leave this field blank.
192.168.1.3_
<Aceptar > <Cancelar >
```

En el caso del WOL se decidió no activar el [WOL](#) (Wake on LAN) debido a que se vio como algo prescindible e innecesario.



```
Do you want to enable WOL for this interface?
< Sí > < No >
```

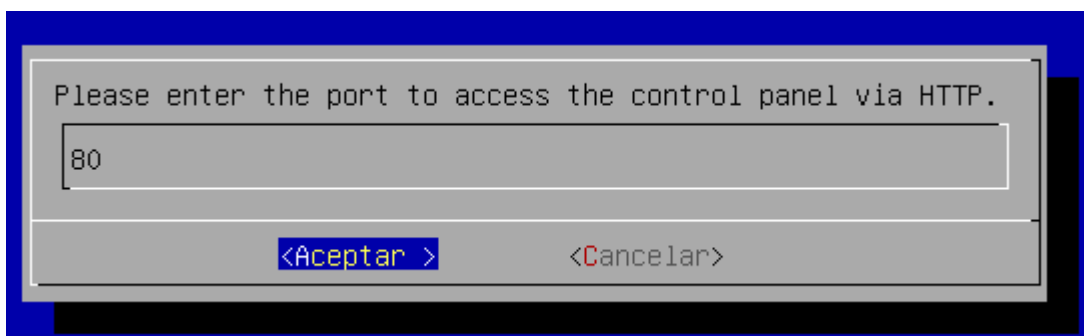
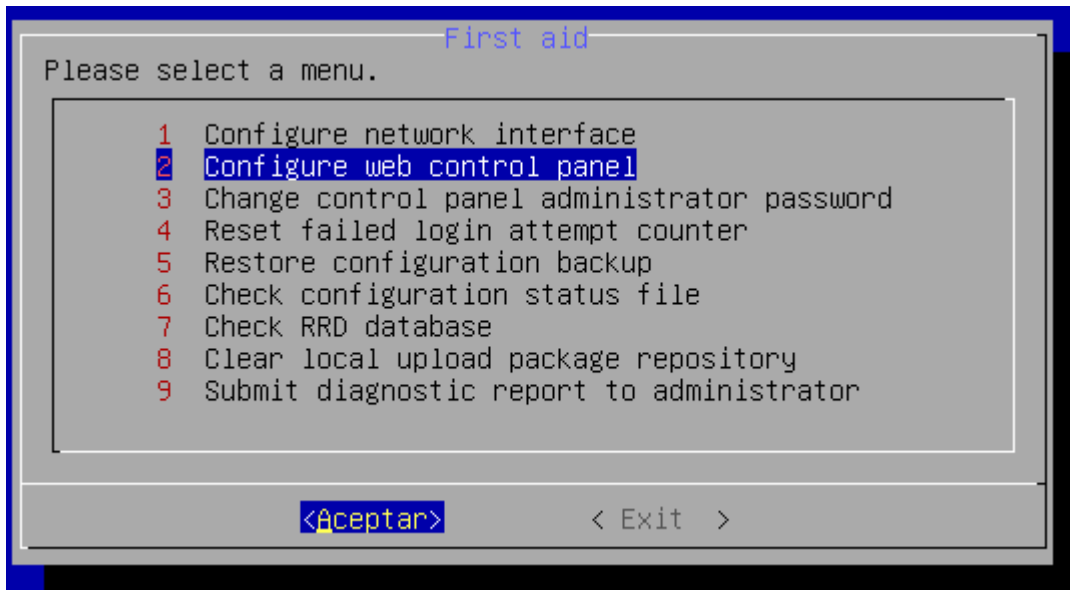
Una vez completada la configuración se guardará y aplicará toda la configuración al darle enter en esta última opción.



Al completar la configuración cuando se consulte la IP se deberá ver la IP configurada previamente, en este caso la 192.168.1.6/24

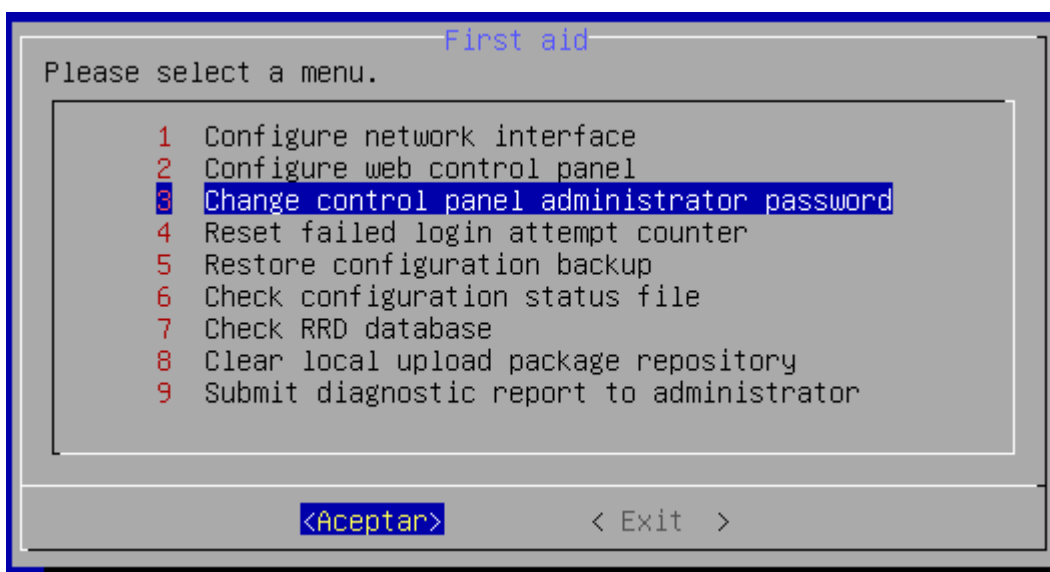
```
root@NAS-proyecto6:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ff:89:c3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.6/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet 192.168.1.34/24 brd 192.168.1.255 scope global secondary dynamic enp0s3
        valid_lft 547sec preferred_lft 547sec
root@NAS-proyecto6:~# _
```

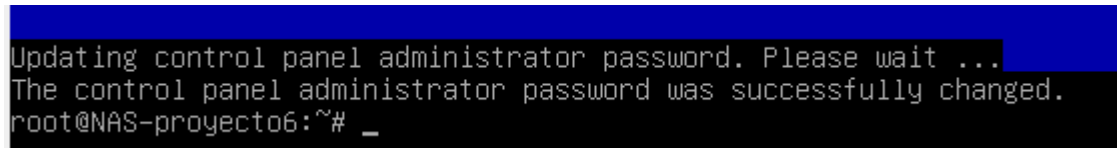
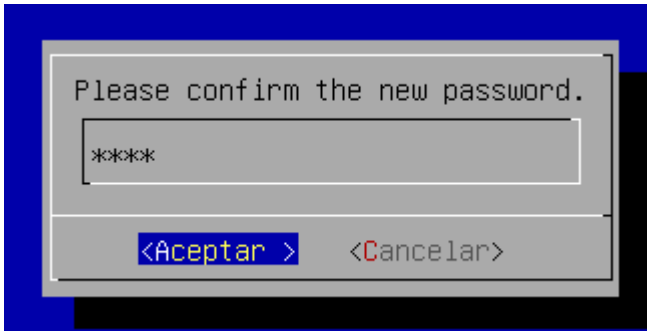
De nuevo se utilizará el comando `omv-firstaid` para reconfigurar otras opciones, entre ellas el puerto que utilizará la interfaz web siendo este por defecto el 80, en este caso se dejará el puerto 80 y se cambiará la contraseña del panel de administración web de Openmediavault que por defecto es `openmediavault` por 1234.



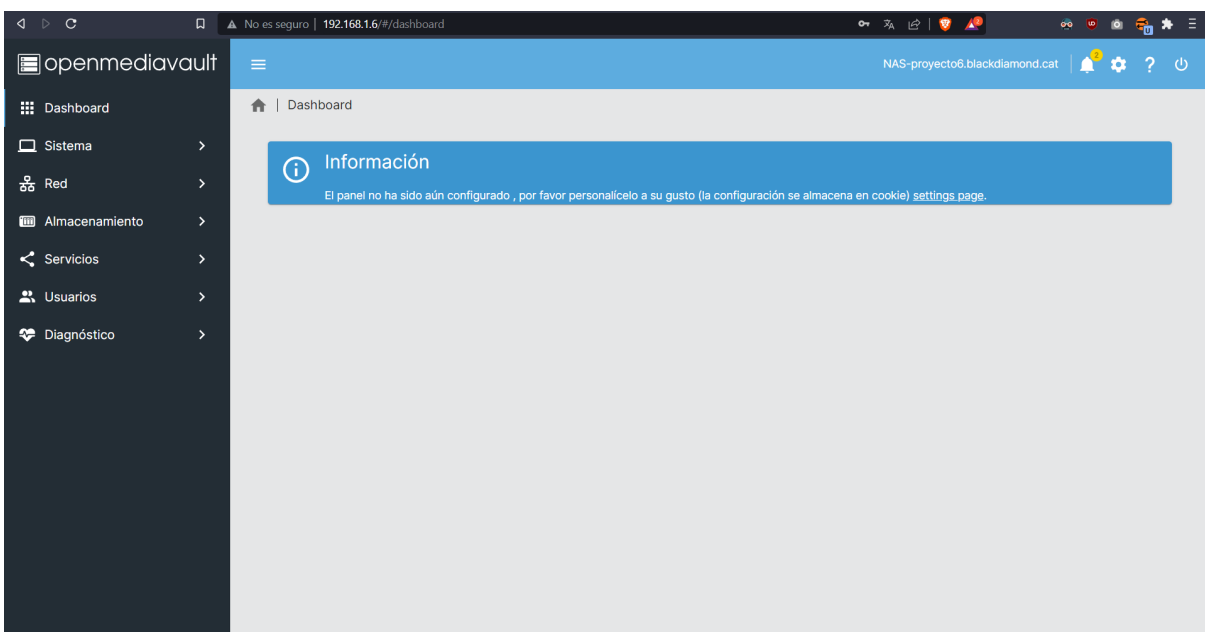
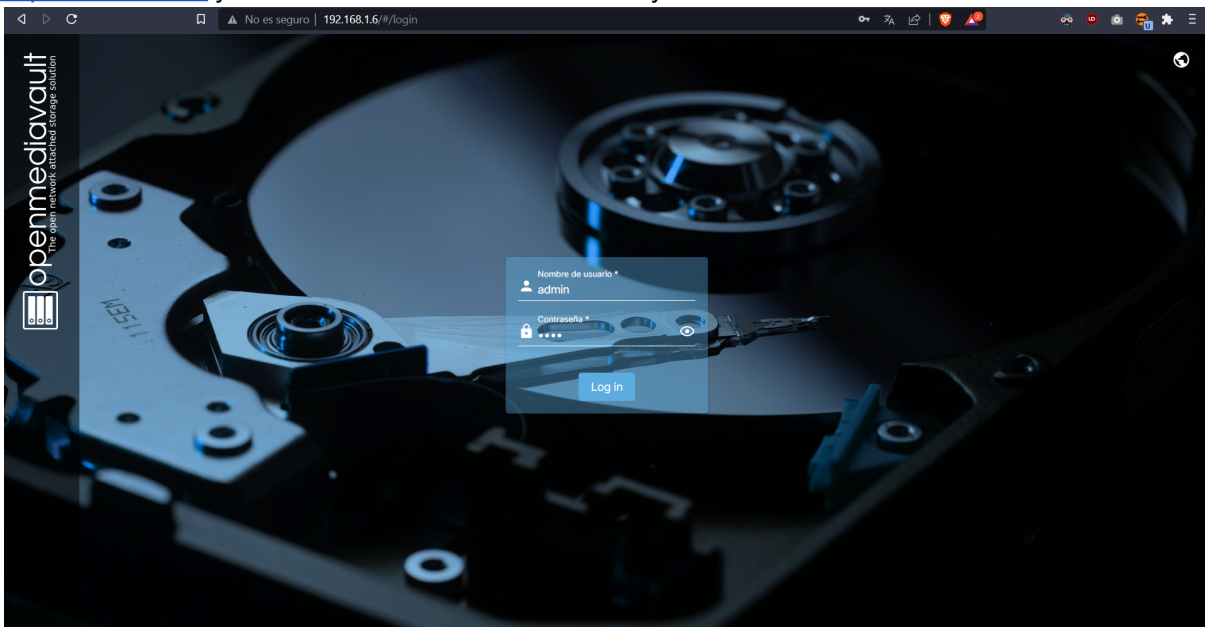
```
Updating web control panel settings. Please wait ...
The web control panel settings were successfully changed.

The web control panel is reachable via URL:
enp0s3: http://192.168.1.6:80
enp0s3: http://192.168.1.34:80
root@NAS-proyecto6:~# _
```

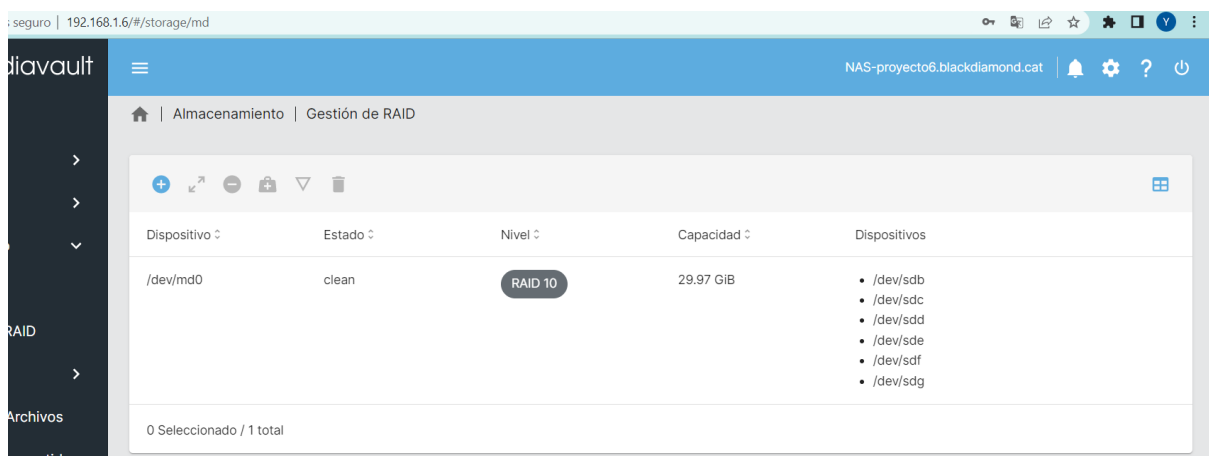
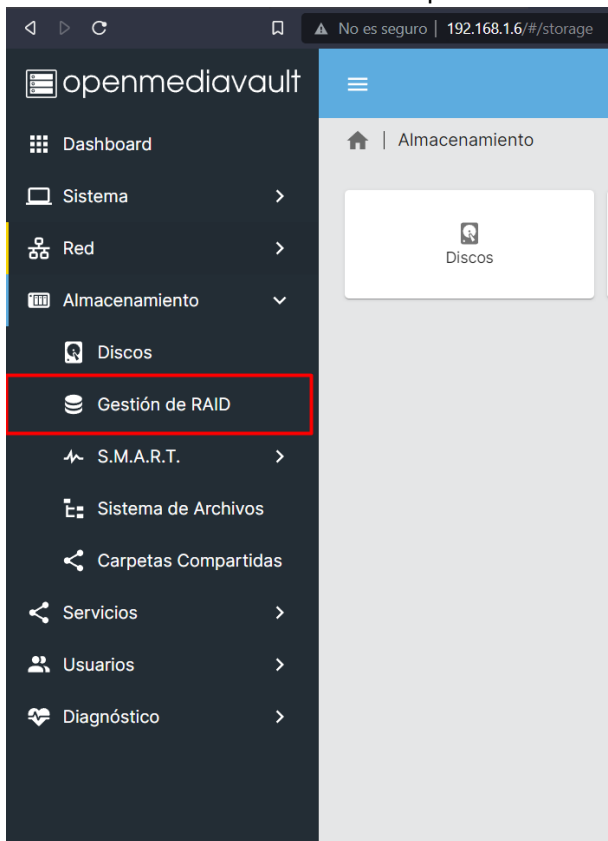




Una vez cambiada y aplicada la configuración se podrá acceder a la interfaz web mediante la IP: <http://192.168.1.6> y se iniciará sesión el usuario admin y la contraseña 1234.

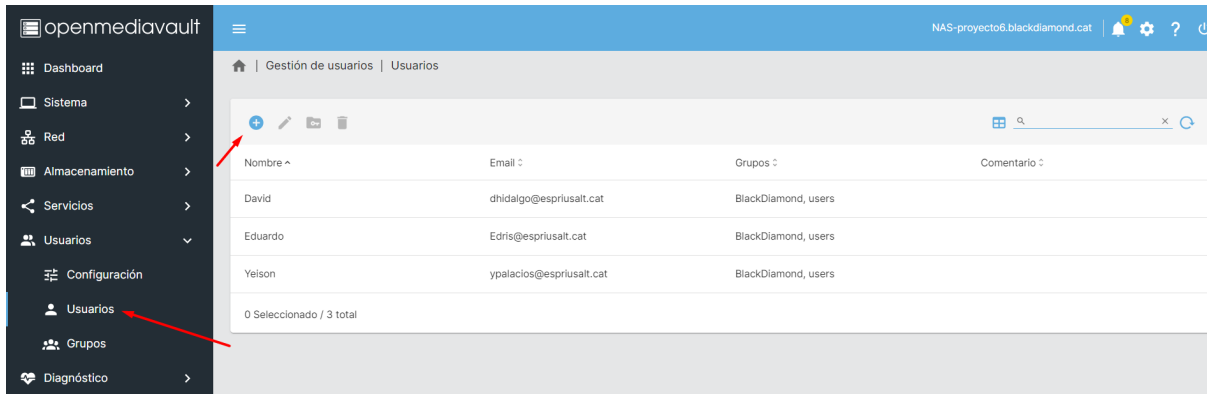


Una vez dentro del panel de control se deberá acceder al menú de creación de los RAID donde se creará el RAID 10 con los 6 discos que se encuentran conectados al NAS.



2- Selecció dels serveis que habilitareu per a que els usuaris de l'empresa puguin compartir recursos centralitzats i en xarxa de dades.

Primero tenemos que añadir los usuarios al OpenMediaVault, esto lo hacemos dándole al apartado de “Usuarios > Usuarios” de la barra de accesos en la parte izquierda de la página.



Llenamos los parámetros necesarios para crear el usuario, tales como, el nombre, email y la contraseña, seguidamente le damos a “Salvar”.

Nombre *
David

Email
dhidalgo@esprisalt.cat

Contraseña *
.....

Confirmar contraseña
.....

Shell
/bin/sh

Grupos
BlackDiamond

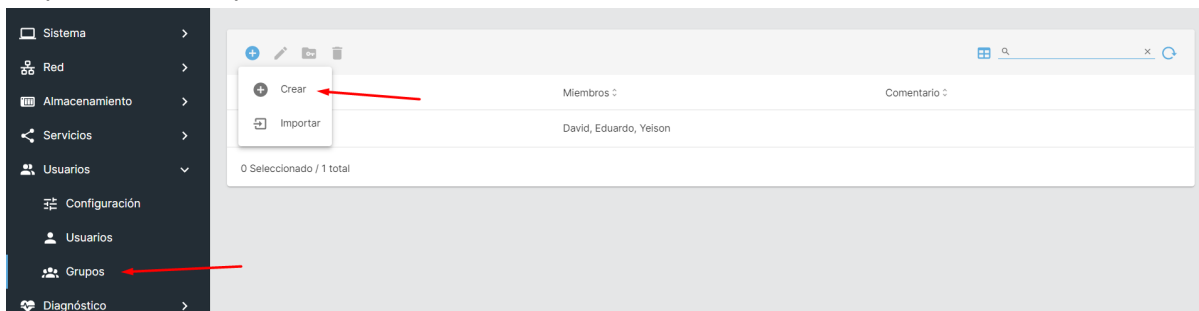
Claves públicas SSH

No hay datos que mostrar.

inhabilita la modificación de la cuenta
inhabilita a un usuario modificar su propia cuenta.
Comentario

Cancelar **Salvar**

Hacemos el mismo proceso que en el paso anterior, pero a diferencia de que tenemos que hacerlo en el apartado de “Grupos”



Dentro ponemos el nombre que queremos ponerle a nuestro grupo y seguidamente tenemos que seleccionar a los usuarios que estarán dentro del grupo.

Nombre *	BlackDiamond
Miembros	David, Eduardo, Yeison
Comentario	
Cancelar Salvar	

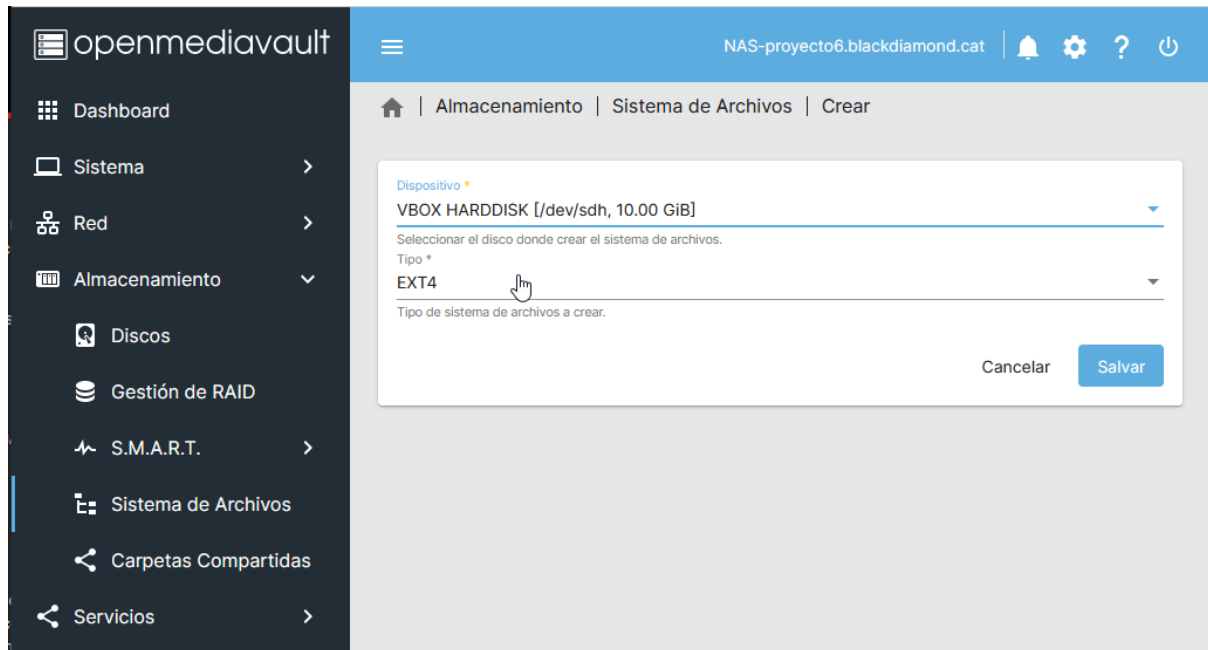
Ahora en el apartado de “Almacenamiento > Sistema de Archivos” tenemos que crear nuestro sistema de archivo para poder compartir la carpeta, para esto tenemos que darle al botón “+” y seguidamente le damos a “Crear”.

The screenshot shows the OpenMediaVault web interface. The left sidebar contains a menu with the following items: Dashboard, Sistema, Red, Almacenamiento, Discos, Gestión de RAID, S.M.A.R.T., Sistema de Archivos, Carpetas Compartidas, Servicios, Usuarios, and Diagnóstico. The main content area is titled 'Almacenamiento | Sistema de Archivos'. It features a table with columns: Disponible, Usado, Montados, Referenciado, and Estado. A red arrow points to the '+ Crear' button in the top left of the table. Another red arrow points to the 'Sistema de Archivos' menu item in the sidebar. The table contains one entry:

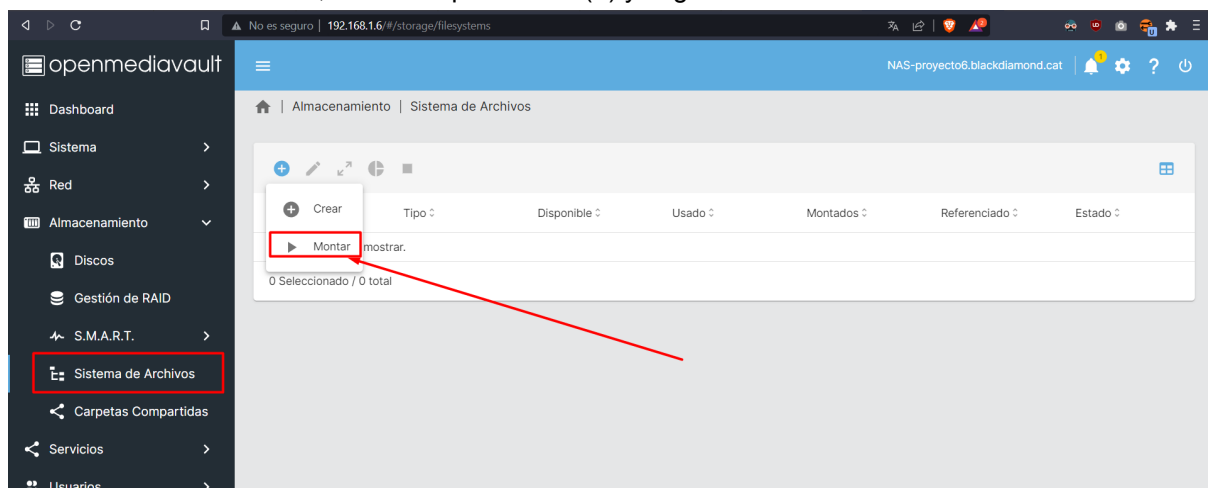
Disponible	Usado	Montados	Referenciado	Estado
29.06 GiB	270.37 M	✓	✓	Online

Below the table, it says '0 Seleccionado / 1 total'.

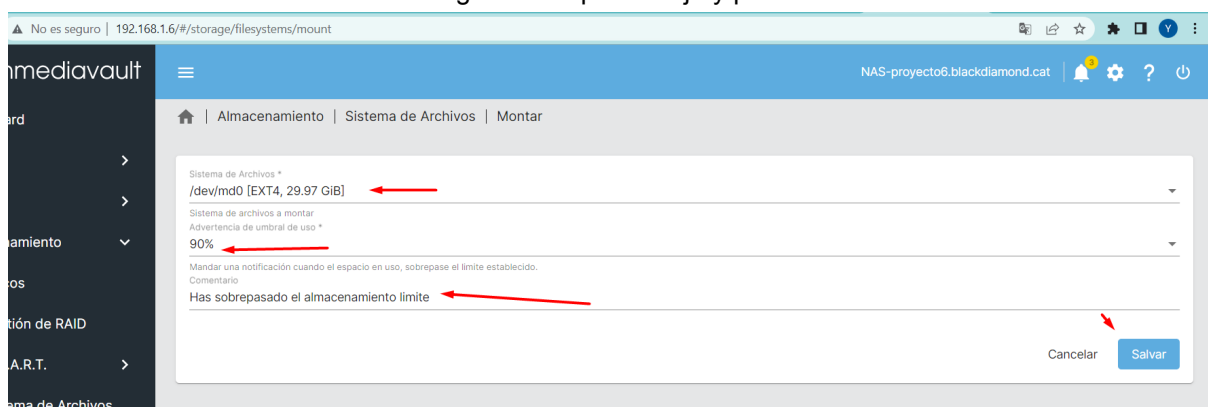
En este menú, deberemos seleccionar el disco que deseemos y el tipo de sistema de archivo.



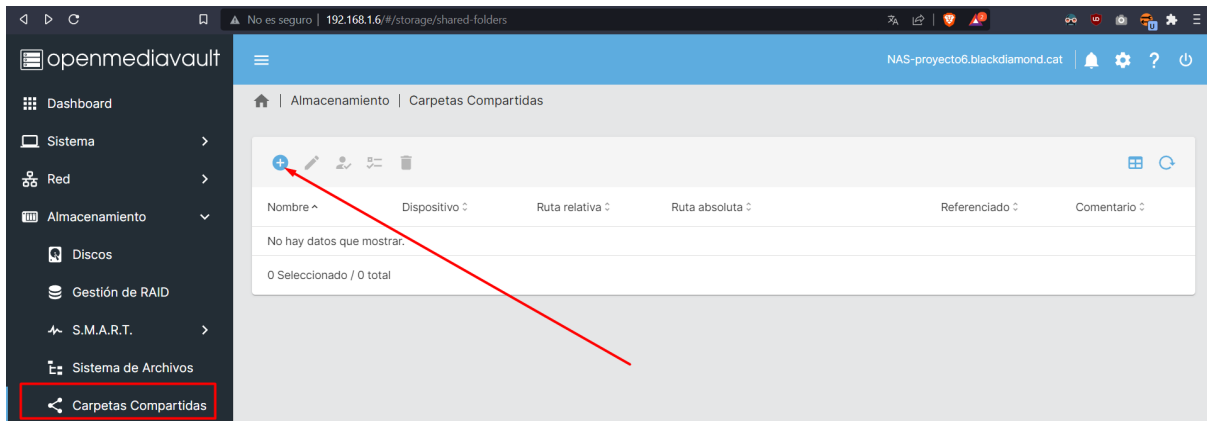
Una vez hecha la creación, tenemos que darle a (+) y seguidamente a “montar”.



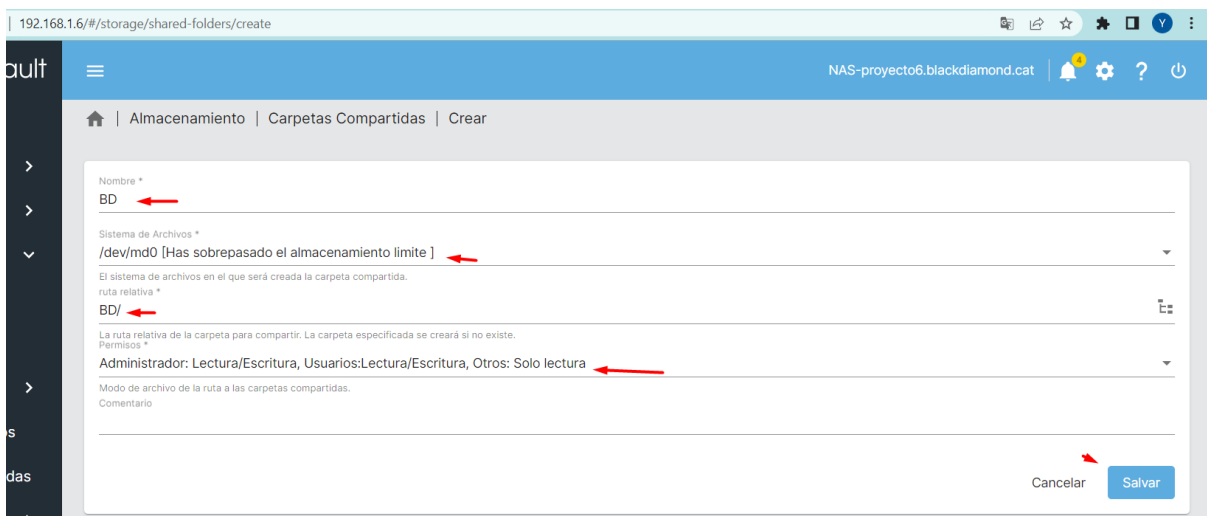
Después seleccionamos el sistema de archivo que hemos creado previamente, ponemos una advertencia de uso cuando el disco llegue a ese porcentaje y ponemos un comentario.



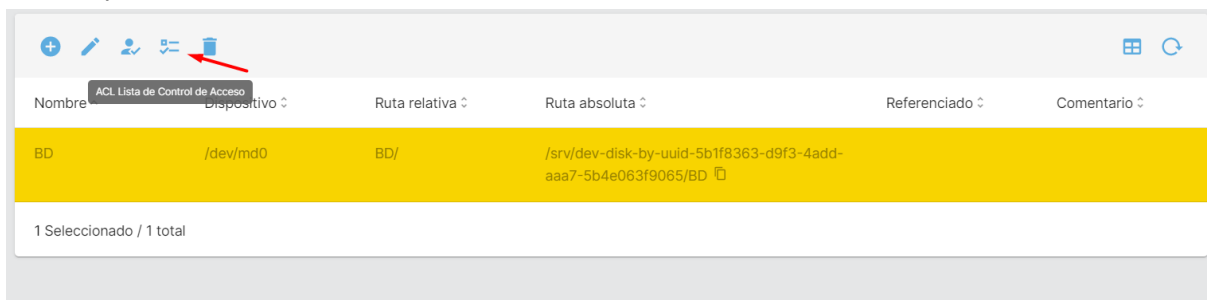
Ahora tenemos que darle al apartado de “Carpetas Compartidas”, tenemos que darle al botón de “+”, para comenzar la creación de la misma.



Ahora nos pedirá el nombre que le pondremos a la carpeta compartida, el sistema de archivo (que es el que creamos en el paso anterior), y los permisos, una vez llenados todos estos parámetros, le damos a “Salvar”.



Seguidamente, seleccionamos el botón de ACL, que es para darle permisos a los usuarios y el grupo creados previamente.



Seleccionamos los permisos que queremos darle a cada usuario y al grupo.

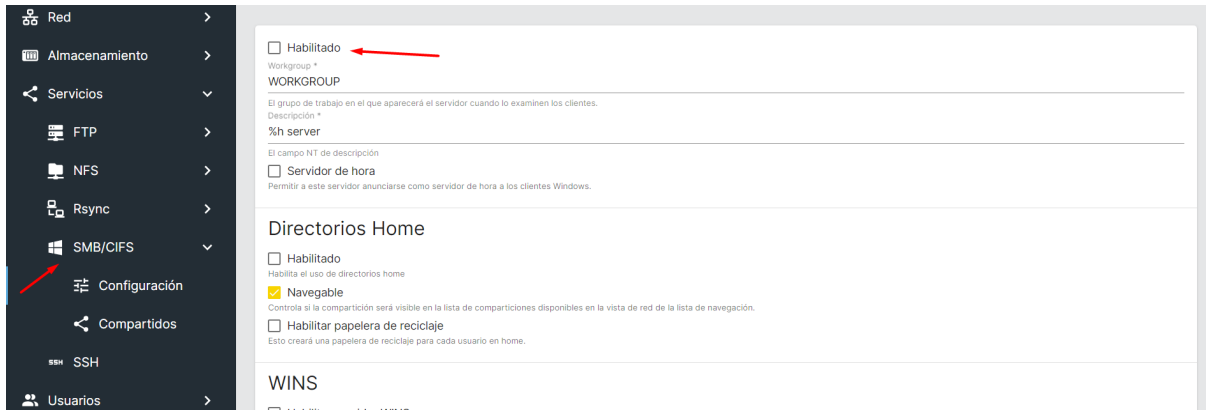
Almacenamiento | Carpetas Compartidas | ACL

Permisos de Usuario/Grupo

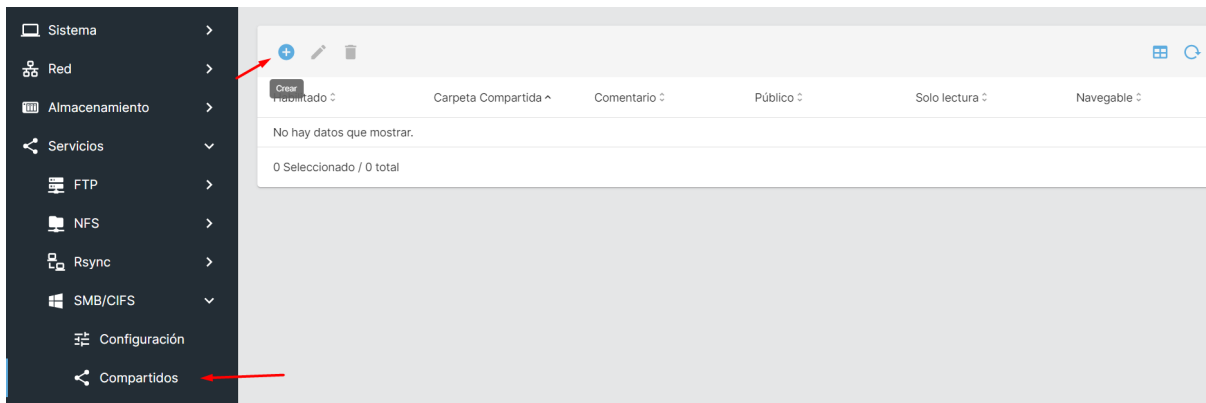
Nombre ^	Tipo ^	Cuenta del sistema ^	Permisos ^
BlackDiamond	Group		<input type="checkbox"/> Read/Write <input checked="" type="checkbox"/> Read-only <input type="checkbox"/> No access
David	User		<input type="checkbox"/> Read/Write <input type="checkbox"/> Read-only <input type="checkbox"/> No access
Eduardo	User		<input type="checkbox"/> Read/Write <input type="checkbox"/> Read-only <input type="checkbox"/> No access
Yeison	User		<input checked="" type="checkbox"/> Read/Write <input type="checkbox"/> Read-only <input type="checkbox"/> No access
._apt	User	✓	<input type="checkbox"/> Read/Write <input type="checkbox"/> Read-only <input type="checkbox"/> No access

3- Guia de configuració dels diferents serveis per entregar-ho al client.

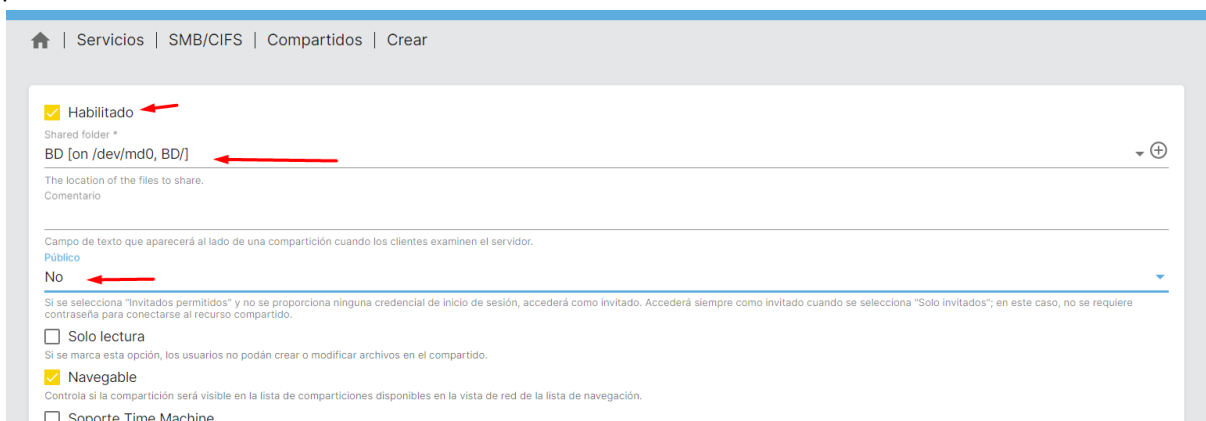
Ahora tenemos que ir al apartado de “Servicios > SMB/CIFS > Configuración” y después tenemos que darle a “habilitar” para activar el servicio.



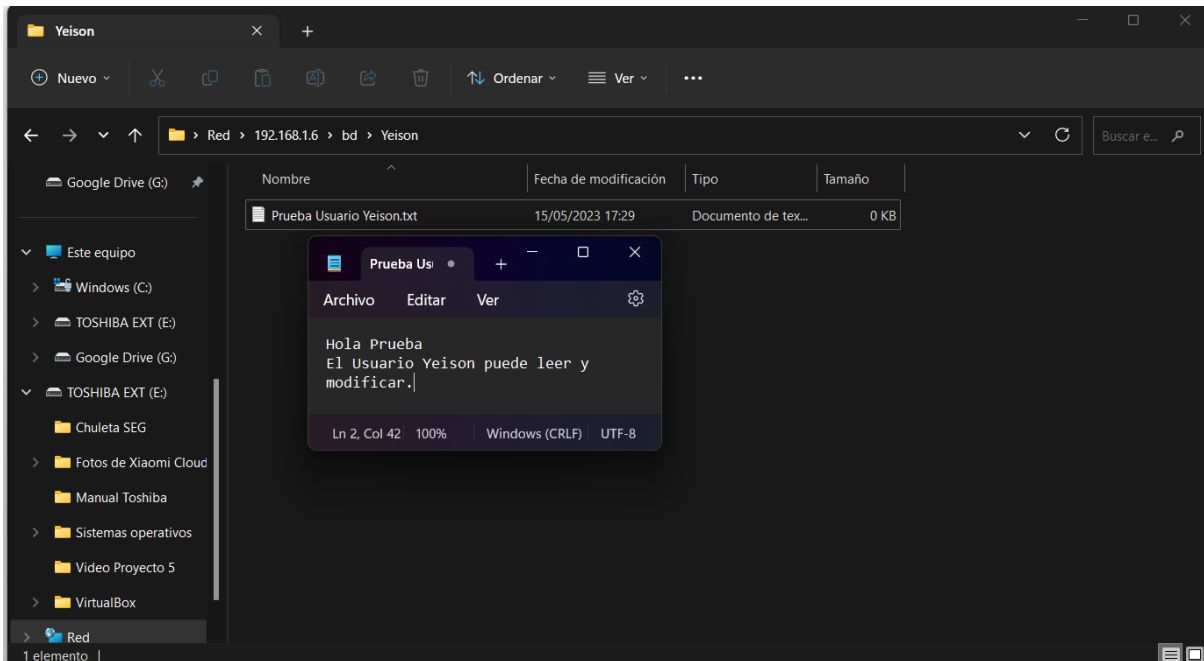
Ahora en el apartado de “compartidos”, tenemos que darle al (+) para seleccionar la carpeta compartida que el servicio va a compartir.



Habilitamos, seleccionamos la carpeta compartida, y finalmente seleccionamos que no esté en pública.



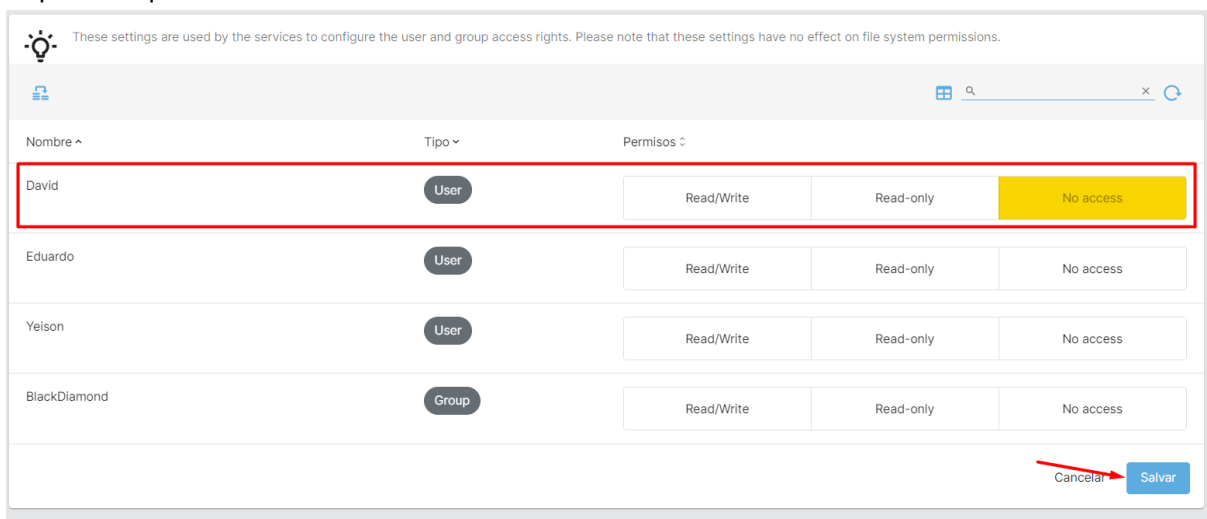
Y ahora podemos ver que nuestra red Green puede conectarse a nuestro servidor de carpetas compartidas.



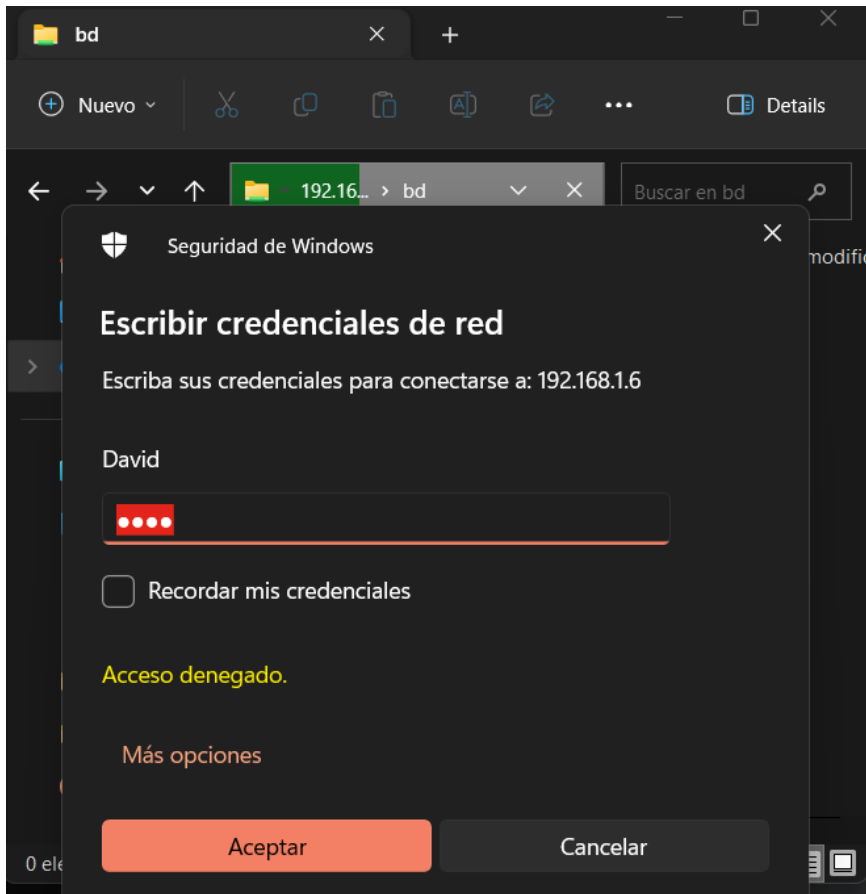
Ahora vamos a modificar los privilegios de la carpeta compartida, esto lo hacemos yendo al botón de "Privilegios".



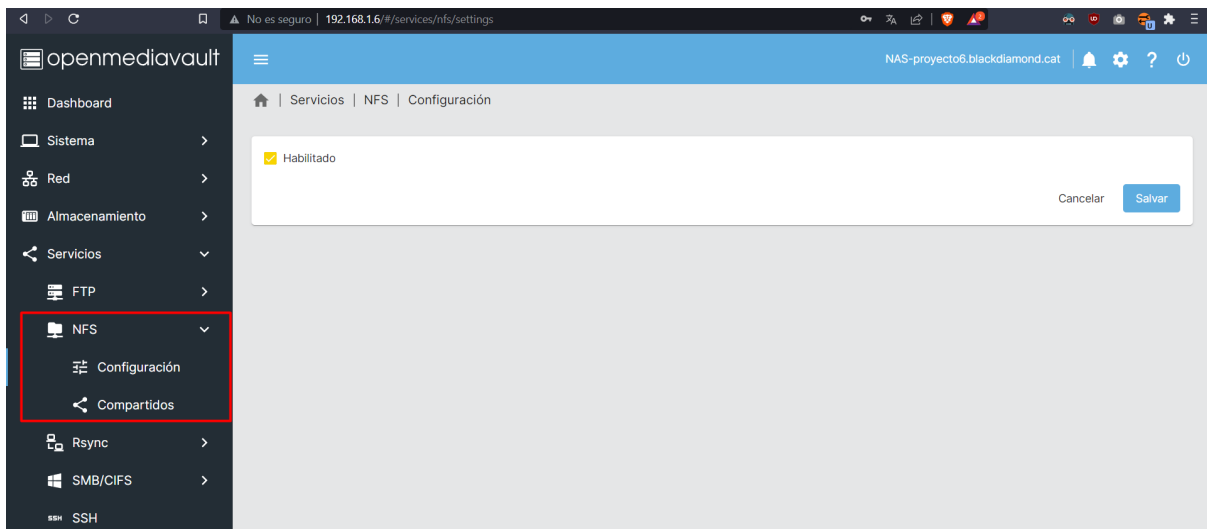
Seguidamente, tenemos que seleccionar el usuario que queremos que no tenga privilegios sobre la carpeta compartida.



Ahora podemos comprobar que los privilegios han funcionado, ya que el usuario que hemos seleccionado, ya no tiene acceso sobre el documento.



Ahora, vamos a iniciar otro servicio, esto lo podemos hacer yendo a “Servicio > NFS > Configuración”, para habilitar otro servicios para compartir, ahora le damos a habilitar y seguidamente a “Salvar”.



Ahora en el apartado de “Compartidos” tenemos que darle a crear y seguidamente tenemos que seleccionar la carpeta compartida que vamos a utilizar, la Ip de la red y los privilegios sobre la carpeta compartida.

Servicios | NFS | Compartidos | Crear

Shared folder *
 BD [on /dev/md0, BD/]

The location of the files to share. The share will be accessible at /export/.

Cliente *
 192.168.1.0/24

Clientes a los que se permite montar el sistema de archivos. Ej: 192.168.178.0/24

Privilegio
 Lectura/Escritura

Opciones extra
 subtree_check,insecure

Por favor vea: [página del manual](#) para más detalles.

Comentario

Cancelar Salvar

Ahora vamos a activar otro servicio en nuestro OpenMediaVault, primero lo que tenemos que hacer es crear o modificar algún usuario.

Gestión de usuarios | Usuarios

Nombre	Email	Grupos	Comentario
David	dhidalgo@espriusalt.cat	BlackDiamond, users	
Eduardo	Edris@espriusalt.cat	BlackDiamond, ssh, users	
Yeison	ypalacios@espriusalt.cat	BlackDiamond, users	

1 Seleccionado / 3 total

Seguidamente tenemos que añadirlo al grupo de "ssh" y salvamos la configuración.

Gestión de usuarios | Usuarios | Editar

Nombre
 Eduardo

Email
 Edris@espriusalt.cat

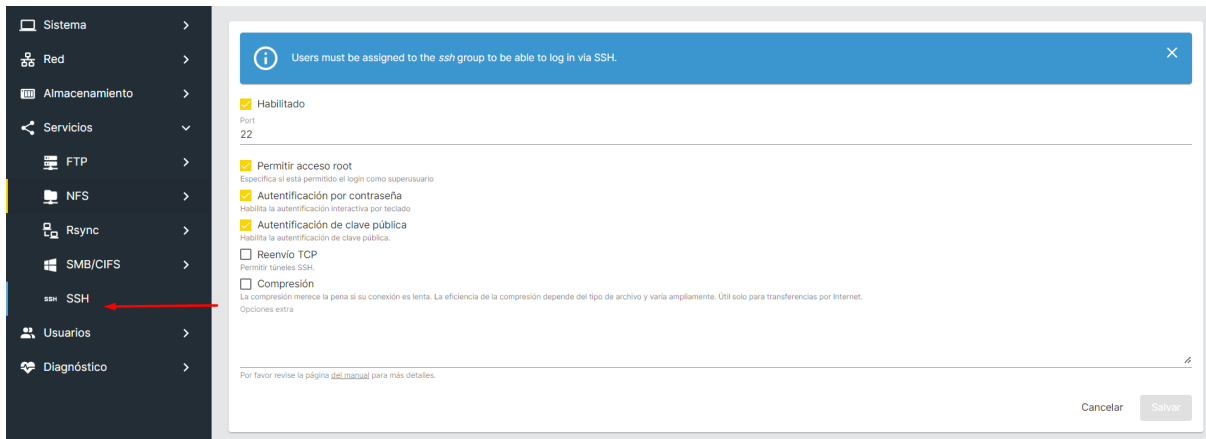
Contraseña

Confirmar contraseña

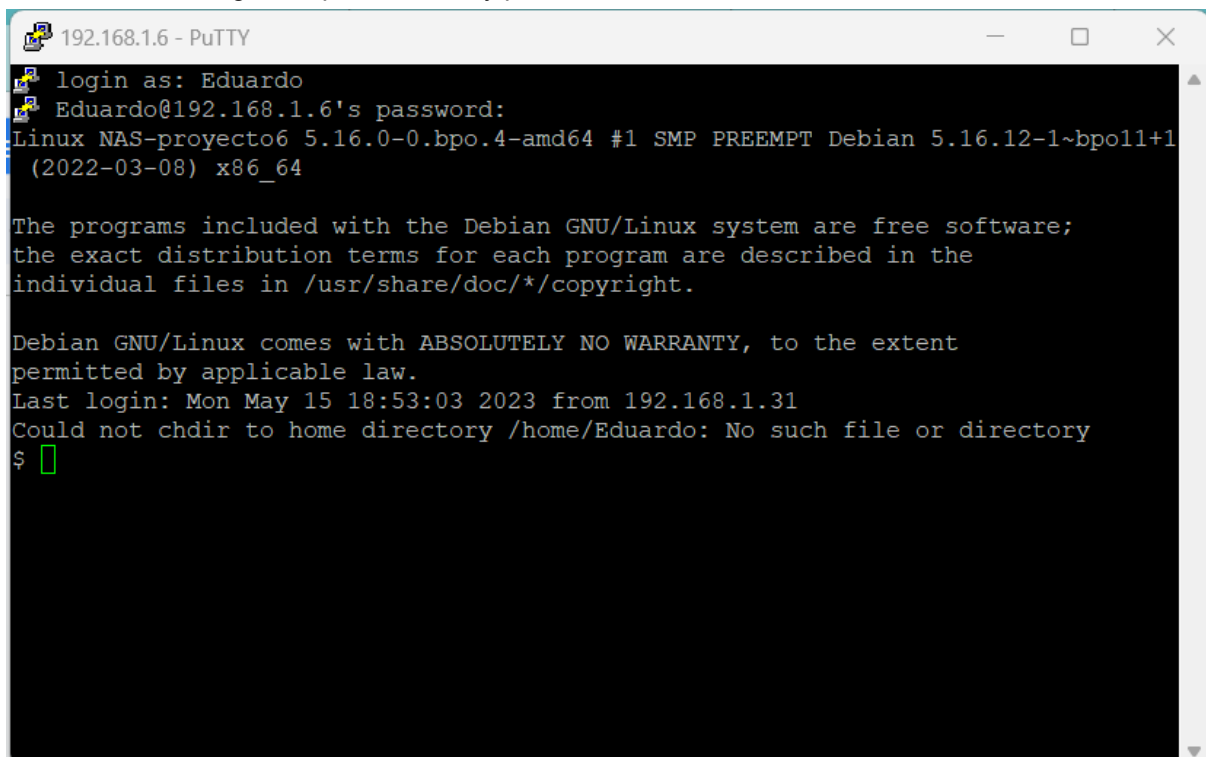
Shell
 /bin/sh

src
 ssh
 ssl-cert
 staff
 sudo
 sys

Verificamos que el servicio del SSH, esté habilitado, yendo a "Servicios > SSH", y si está deshabilitado, lo habilitamos.



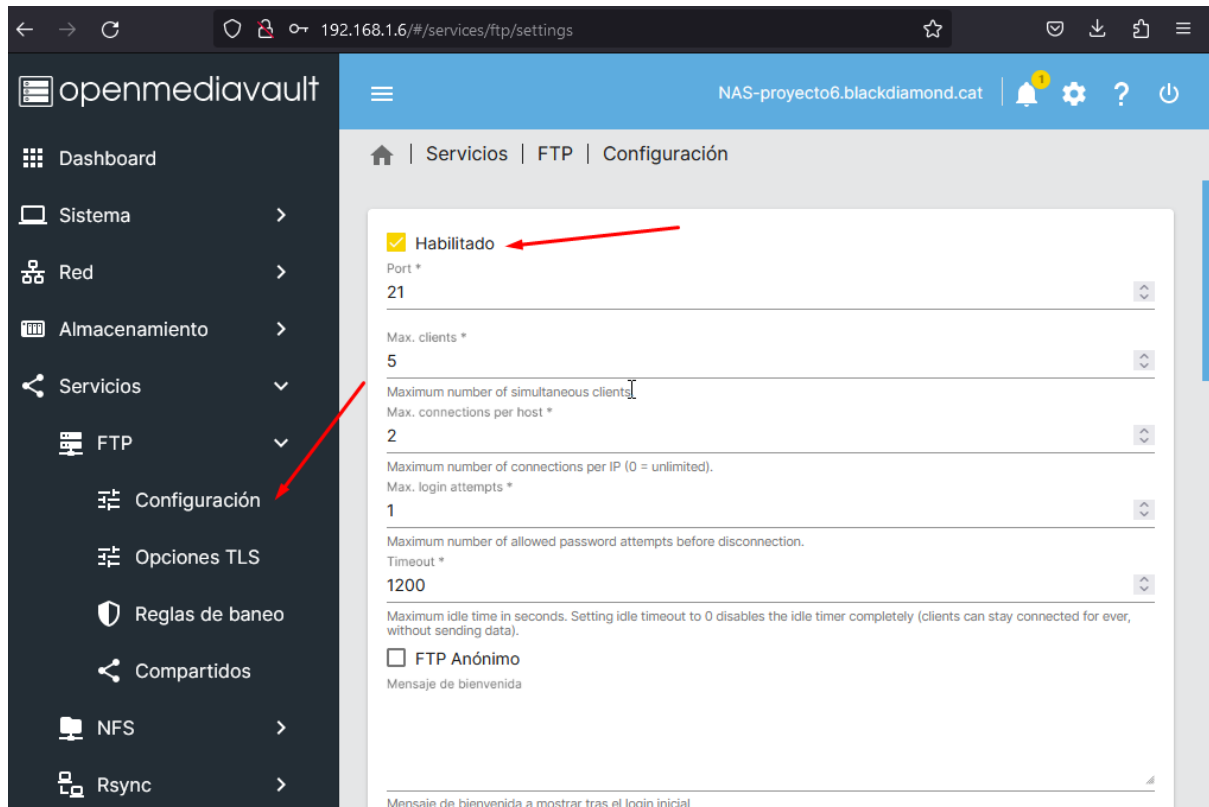
Finalmente podemos comprobar desde el programa PuTTY, podemos conectarnos a nuestro servidor con el usuario configurado previamente, y ponemos la contraseña del mismo.



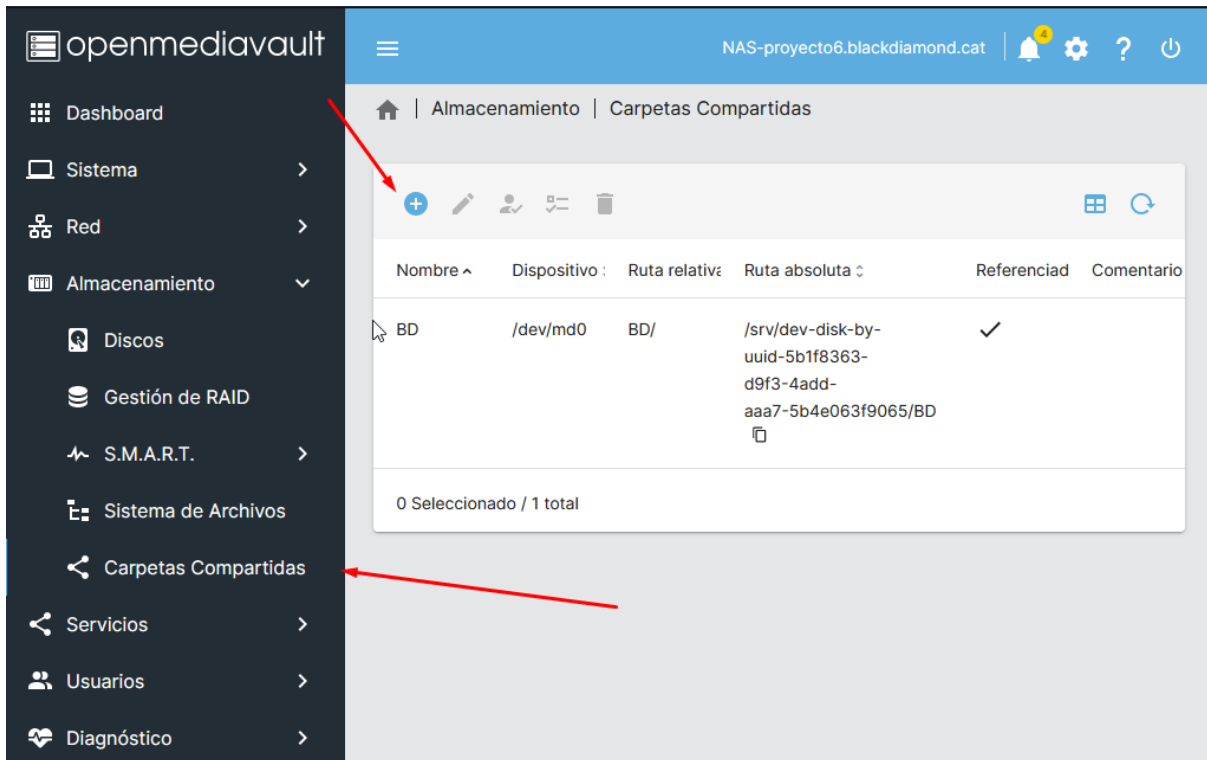
Fase 4 – Configuració de backups i hardening (3h)

1- Configuració dels backups de les dades en un disc en xarxa.

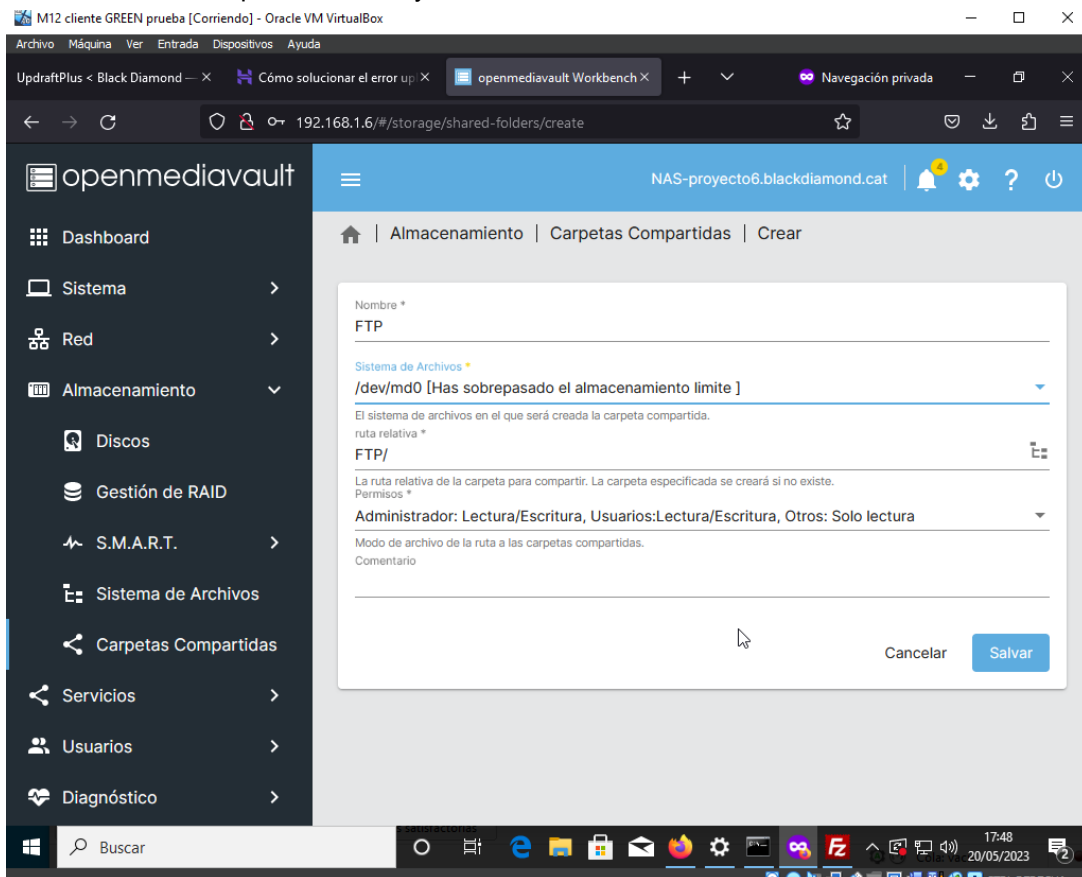
Primero, deberemos habilitar el servicio de FTP en el NAS, para poder hacer las copias de seguridad del WordPress a través de FTP.



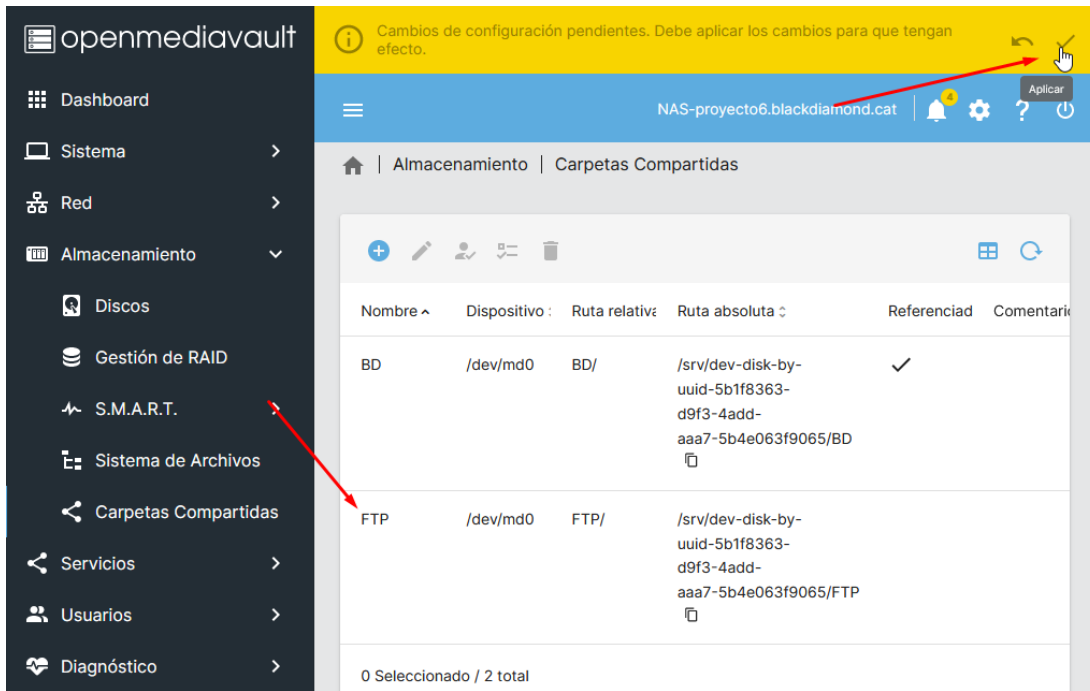
Crearemos una nueva carpeta compartida, para el servicio de FTP.



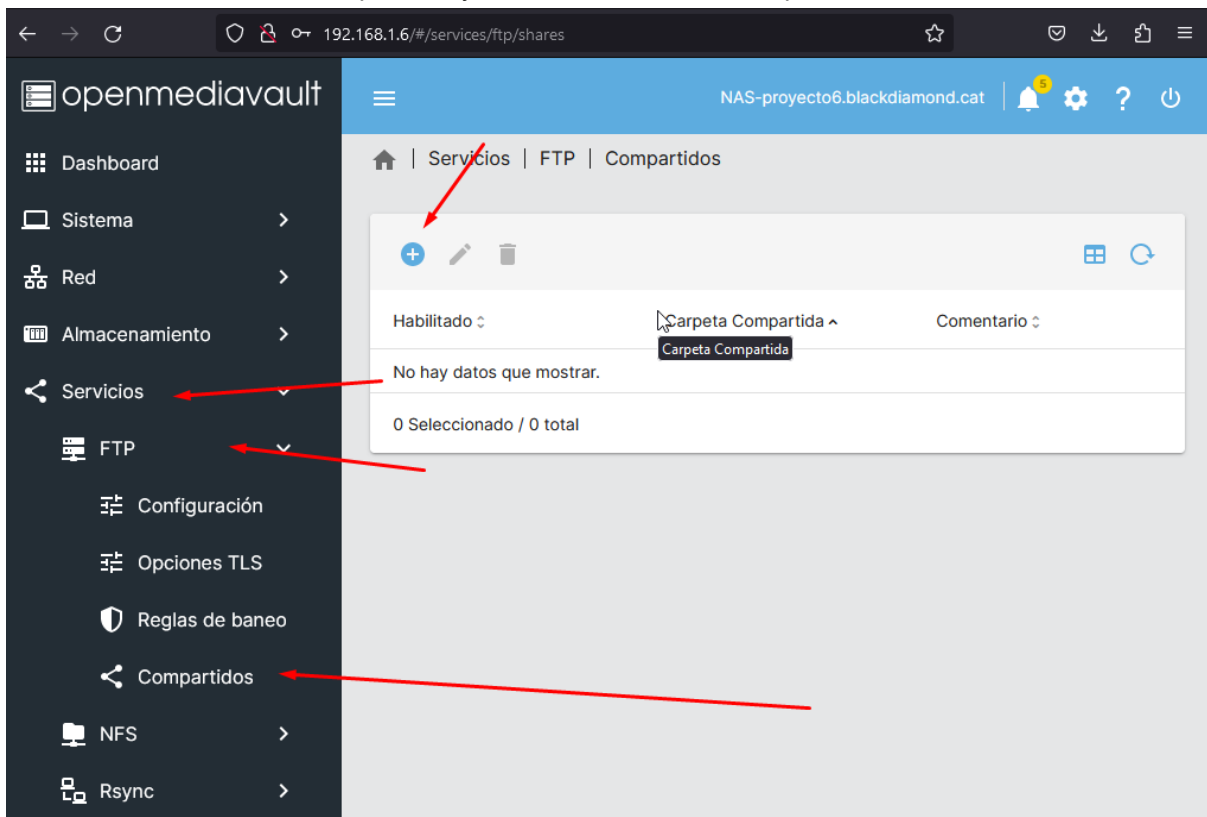
Especificaremos el nombre de la carpeta compartida, "FTP" en este caso, seleccionaremos el sistema de archivo que deseamos y le daremos a salvar.



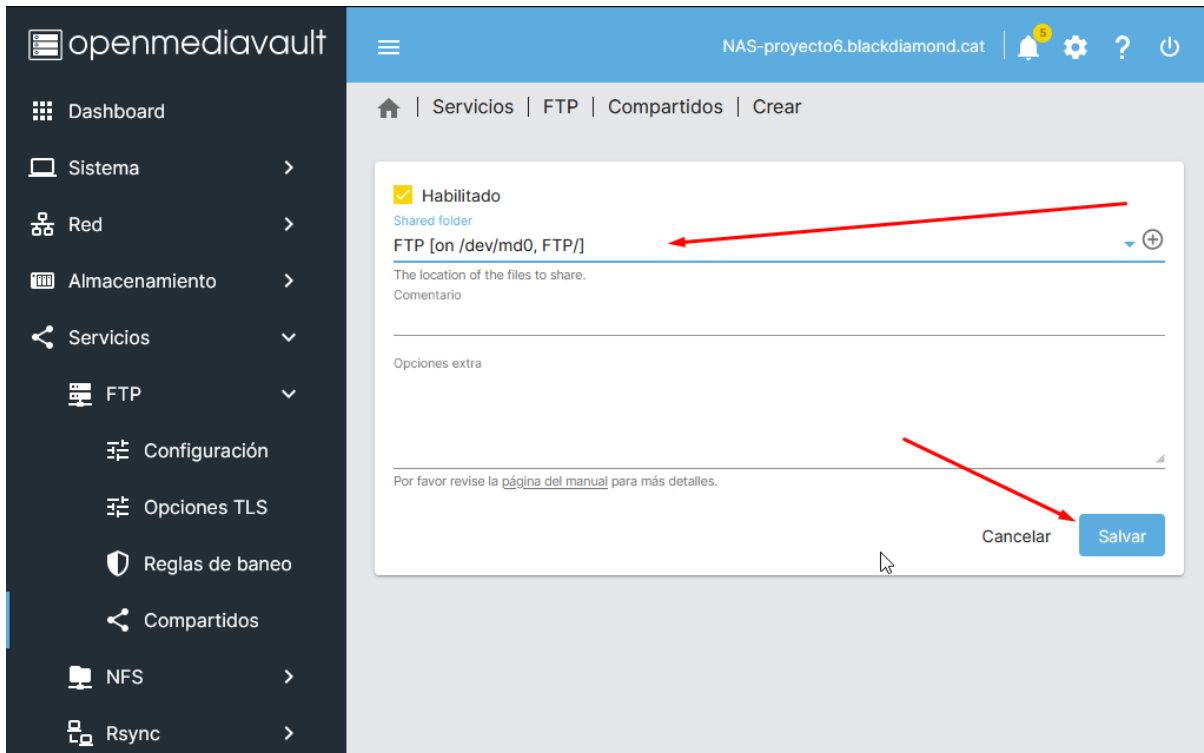
Aplicaremos los cambios una vez realizados.



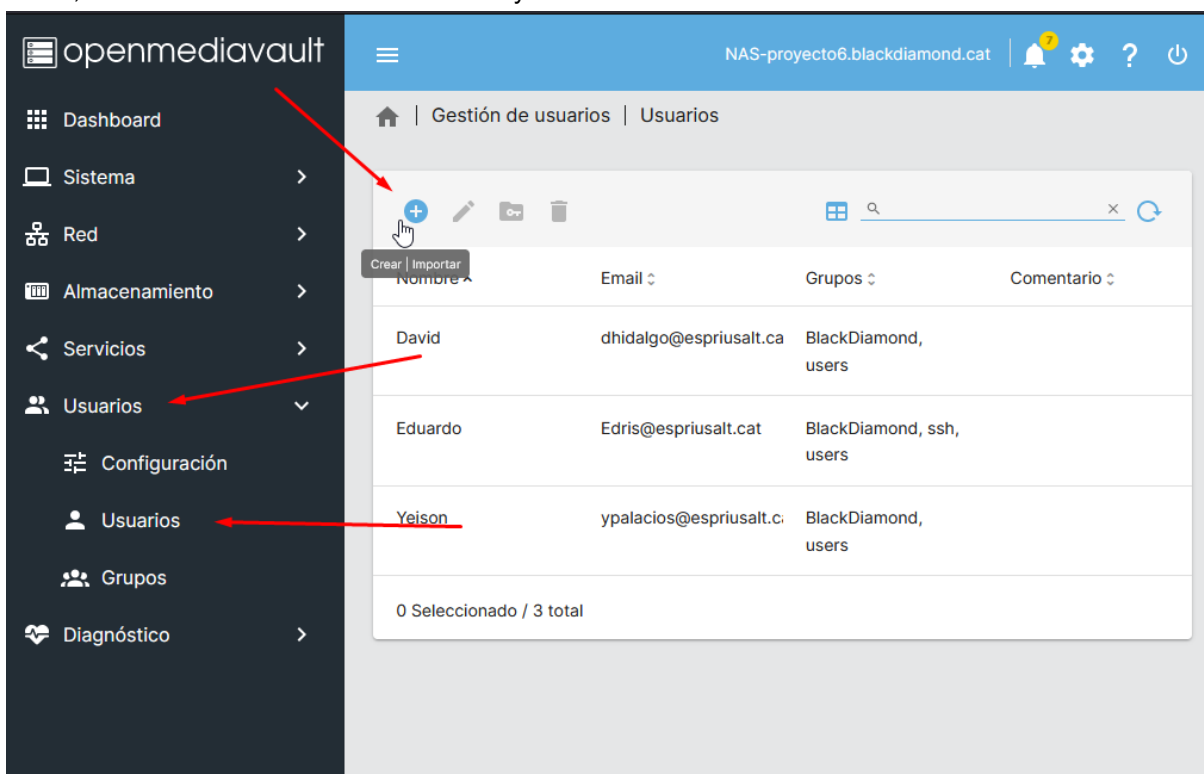
Iremos a Servicios>FTP>Compartidos y crearemos una nueva carpeta.



Seleccionaremos la carpeta que hemos creado anteriormente y le daremos a Salvar.



Ahora, iremos a Usuarios>Usuarios>Crear y crearemos un nuevo usuario.



El usuario se llamará UsuarioBackup y se utilizará solamente para la realización de las Backups.

openmediavault

NAS-proyecto6.blackdiamond.cat

Gestión de usuarios | Usuarios | Crear

Nombre *
UsuarioBackup

Email

Contraseña *
●●●●

Confirmar contraseña
●●●●

Shell
/bin/sh

Grupos
Seleccionar grupos ...

Claves públicas SSH

No hay datos que mostrar.

Una vez creado, modificaremos sus permisos de las carpetas.

openmediavault

Cambios de configuración pendientes. Debe aplicar los cambios para que tengan efecto.

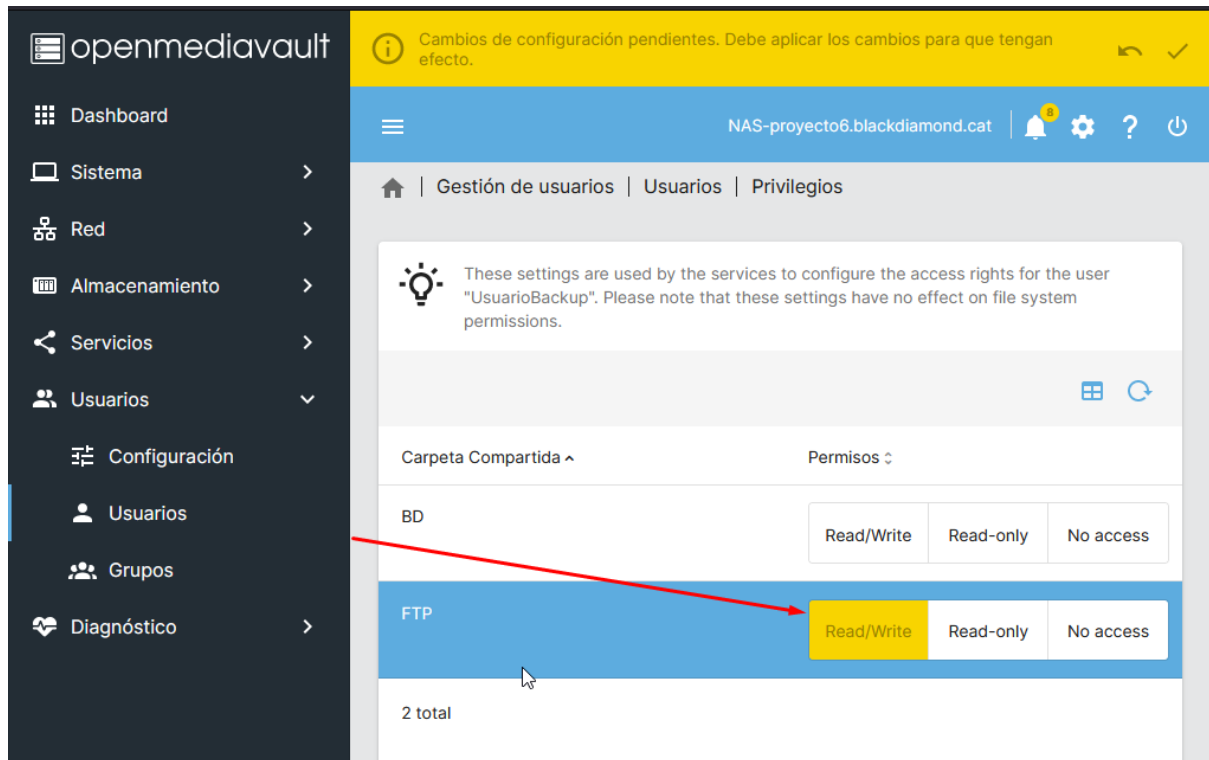
NAS-proyecto6.blackdiamond.cat

Gestión de usuarios | Usuarios

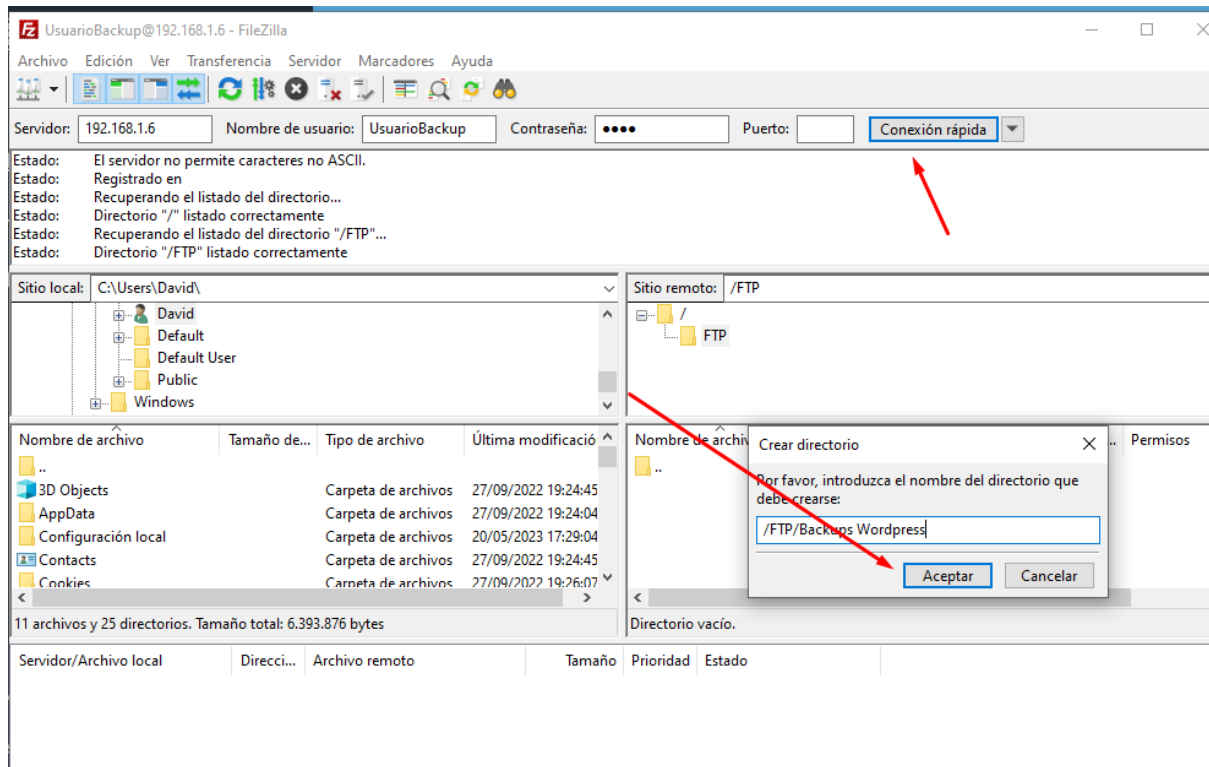
Nombre ^	Email ↕	Grupos ↕	Comentario ↕
David	dhidalgo@espriusalt.ca	BlackDiamond, users	
Eduardo	Edris@espriusalt.cat	BlackDiamond, ssh, users	
UsuarioBackup		users	
Yeison	ypalacios@espriusalt.c	BlackDiamond, users	

1 Seleccionado / 4 total

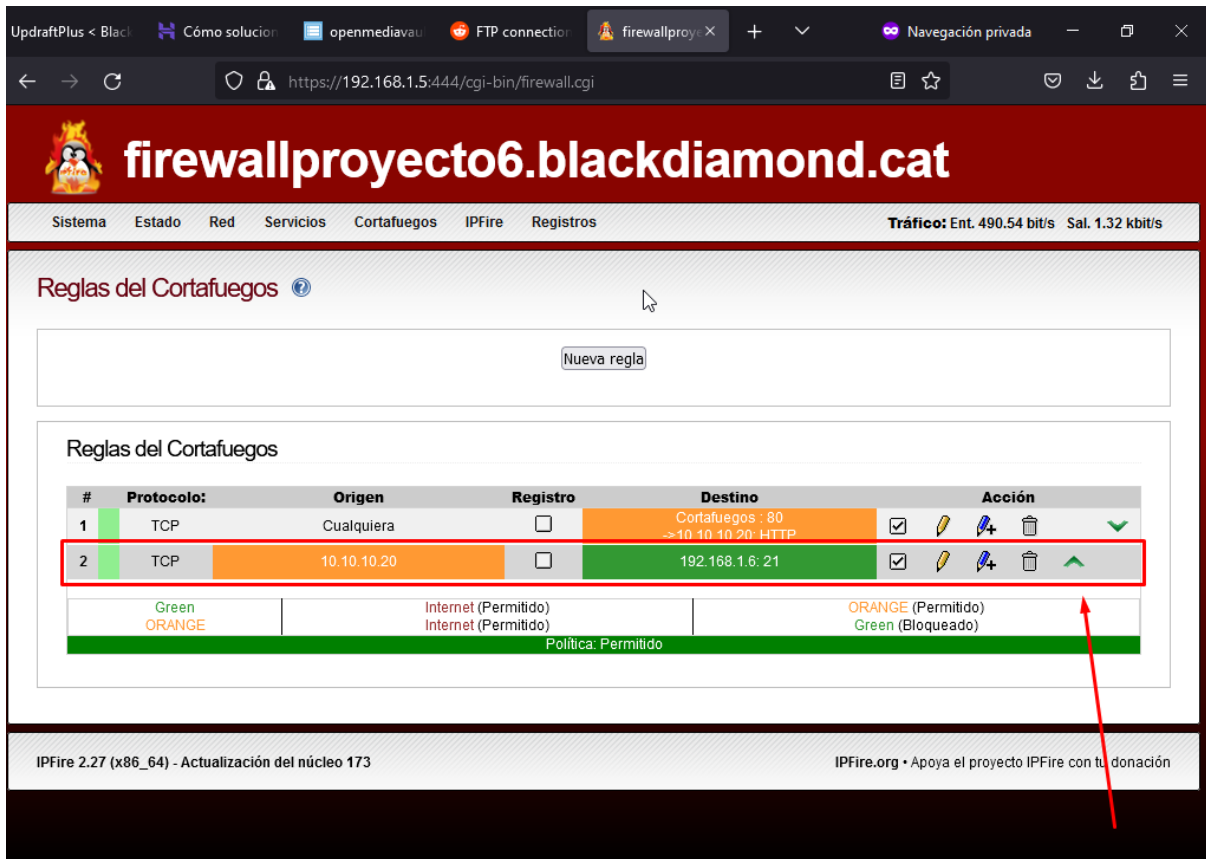
En la carpeta de FTP, le pondremos Read/Write para que tenga permisos de lectura y escritura. Una vez hecho esto, aplicaremos los cambios.



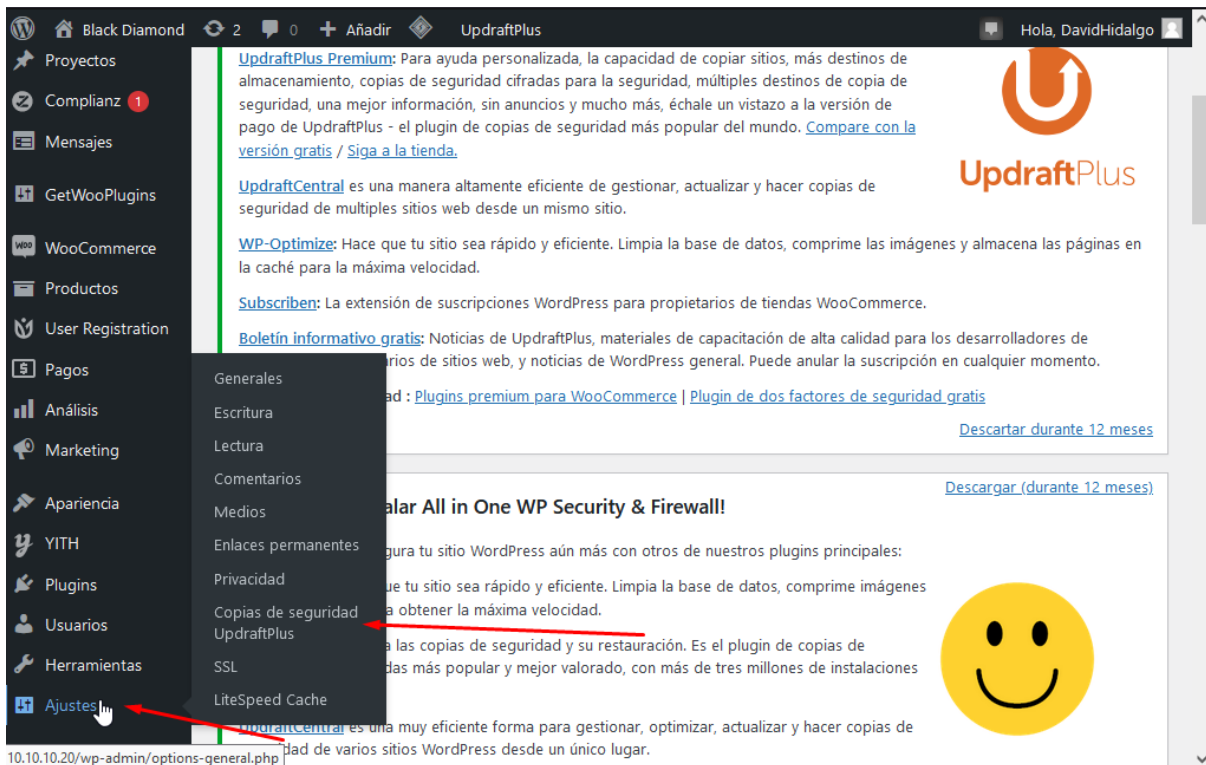
Entraremos por FTP al servidor y crearemos una carpeta para los backups.



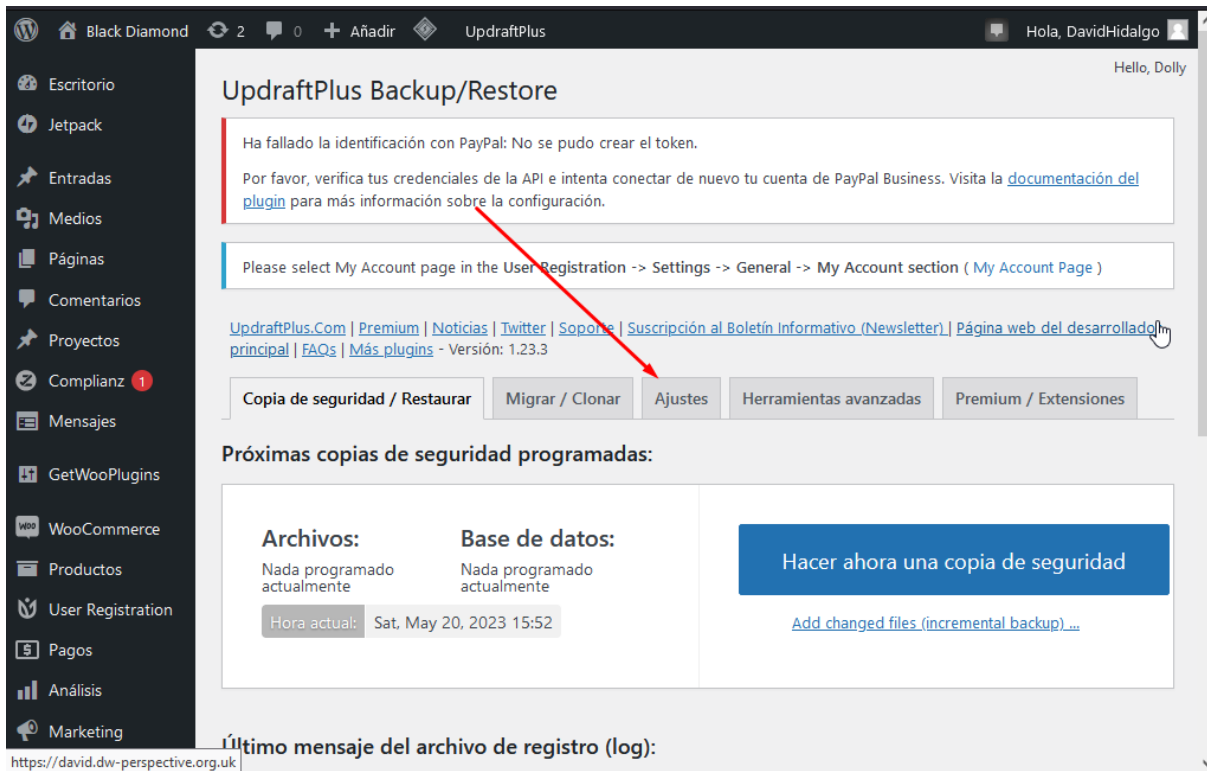
También tendremos que añadir una regla en el firewall, para que la página web se pueda comunicar con el servidor NAS y poder guardar las copias de seguridad a través de FTP (puerto 21).



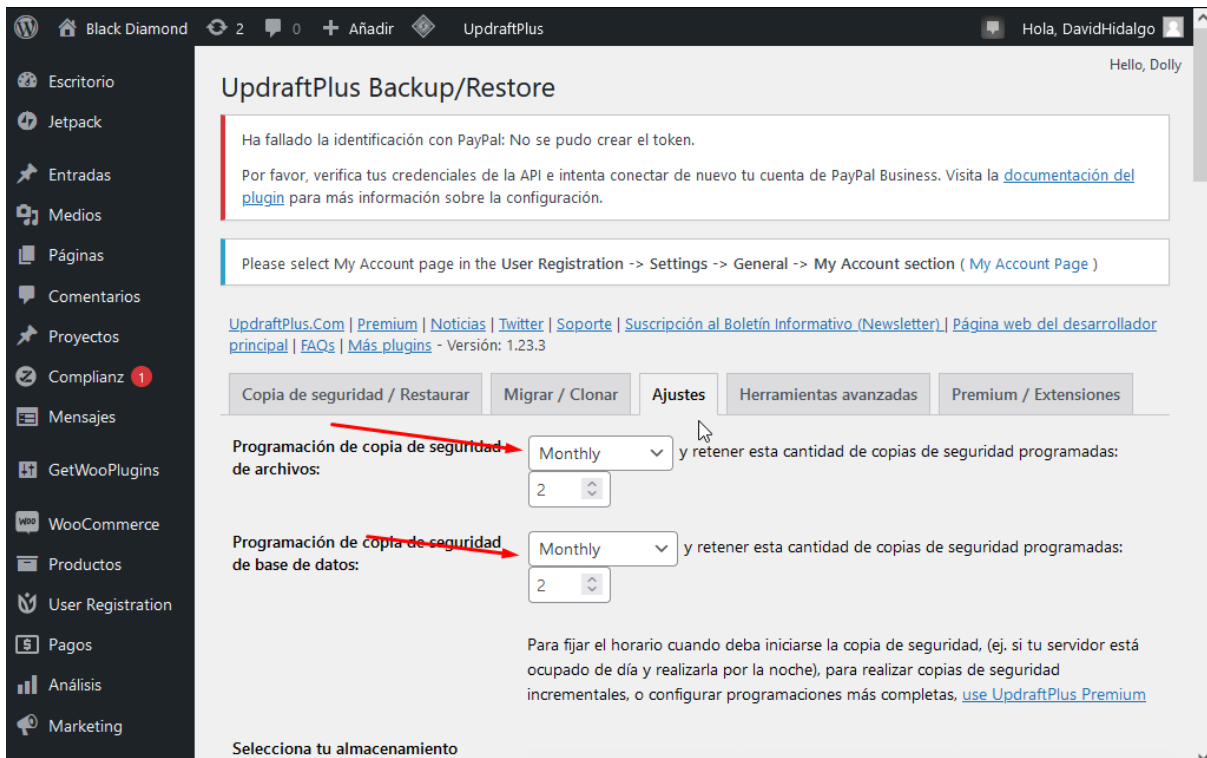
Ahora, iremos a nuestra Web y entramos a la configuración del plug-in “UpdraftPlus”, que instalamos en el Proyecto 4.



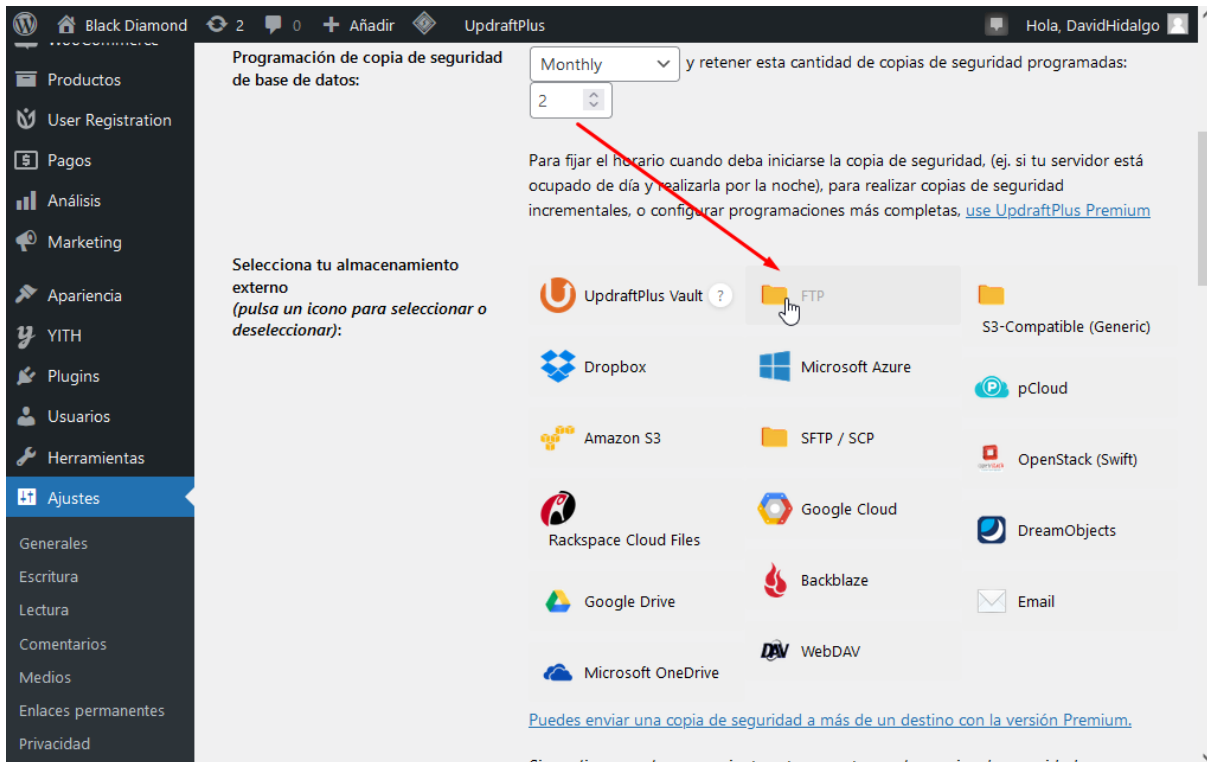
Iremos al apartado de Ajustes.



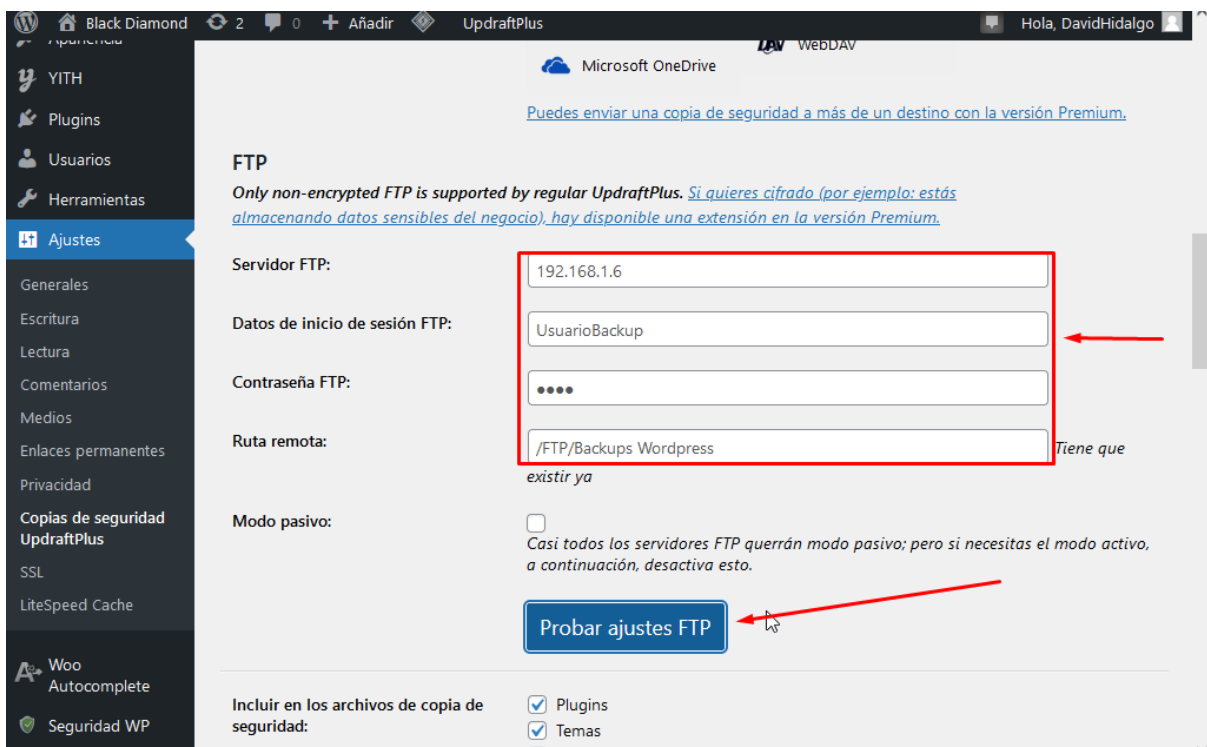
Programaremos la copia de seguridad de los archivos y las bases de datos en "Monthly" para que se hagan mensualmente.



Bajaremos en el mismo menú y encontraremos la opción de "Selecciona tu almacenamiento externo" donde especificaremos FTP.



Si bajamos un poco más, veremos los ajustes para FTP, donde deberemos poner las credenciales del servidor NAS, el usuario y contraseña que hemos creado anteriormente y la Ruta remota donde queremos que se guarden las copias. Le daremos a Probar ajustes FTP, para asegurarnos de que tiene conexión.



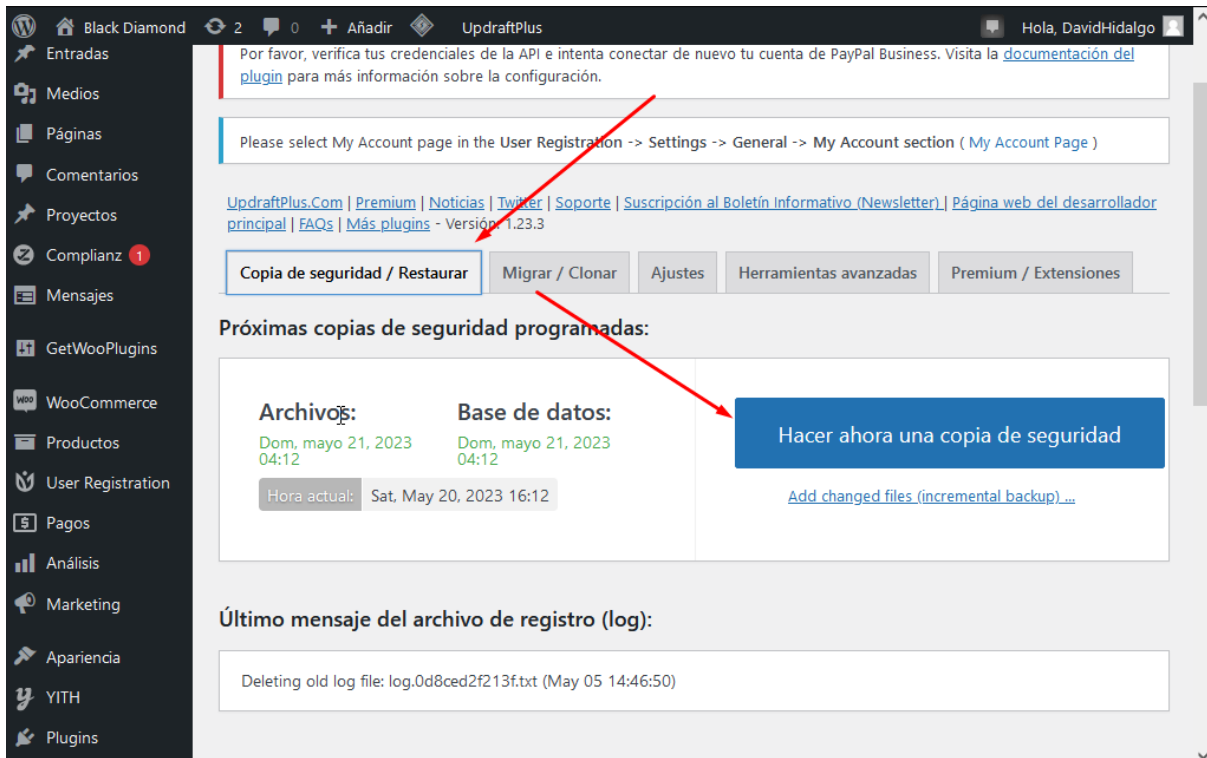
Nos deberá de salir un pop-up que nos avisará de que las credenciales son correctas y se ha iniciado sesión correctamente.



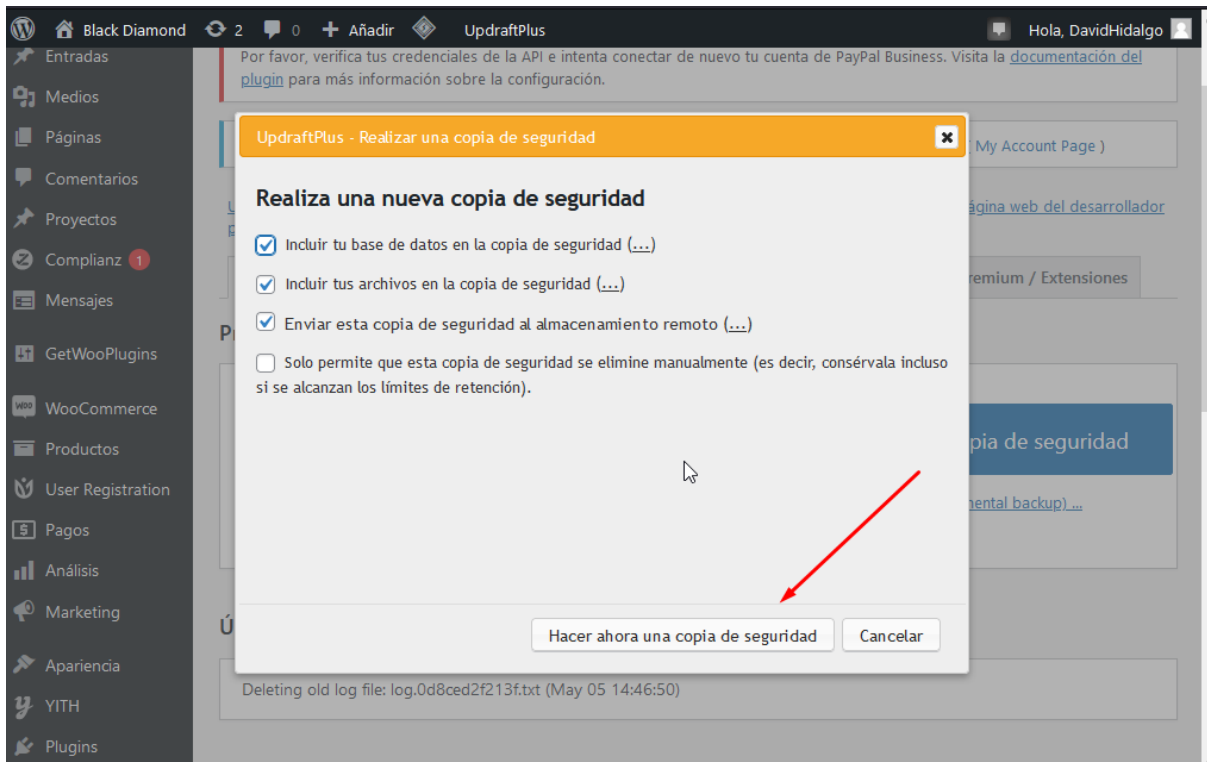
Bajaremos hasta abajo del todo y le daremos a Guardar cambios.



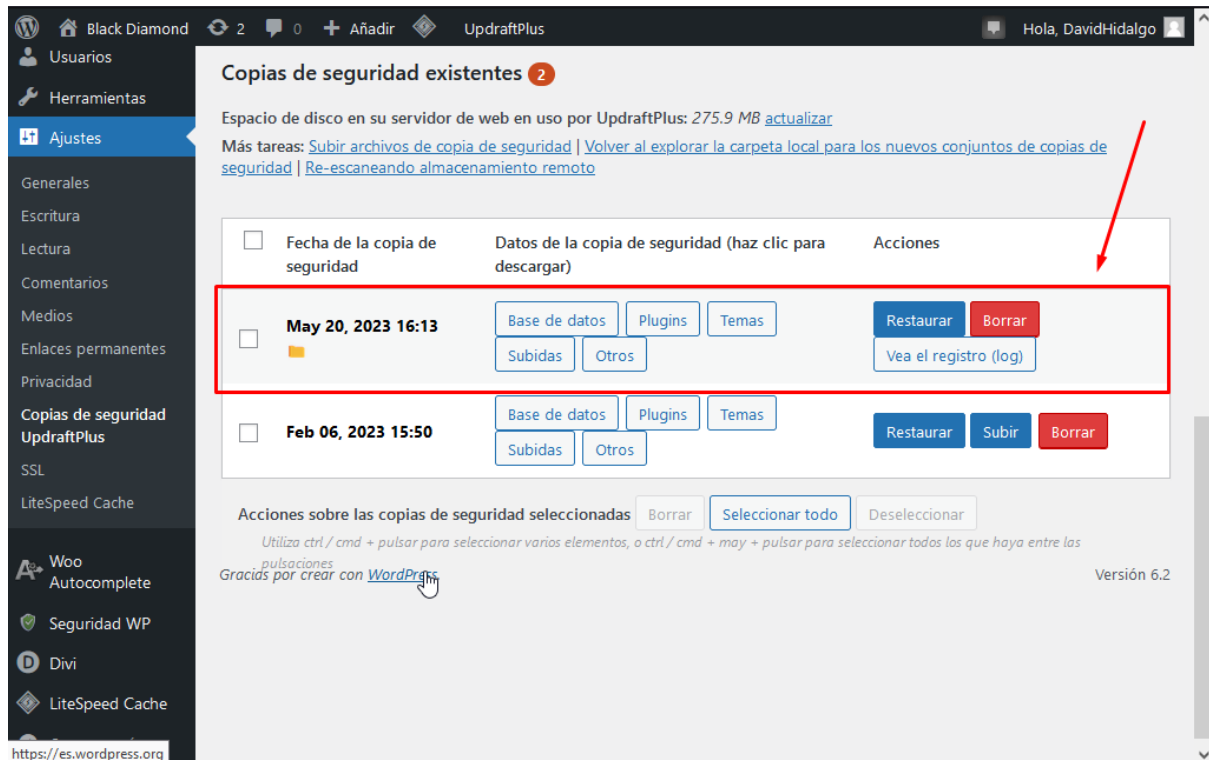
Ahora, probaremos el funcionamiento de las copias de seguridad. Para eso, iremos al apartado de “Copias de seguridad / Restaurar” y le daremos a “Hacer ahora una copia de seguridad”.



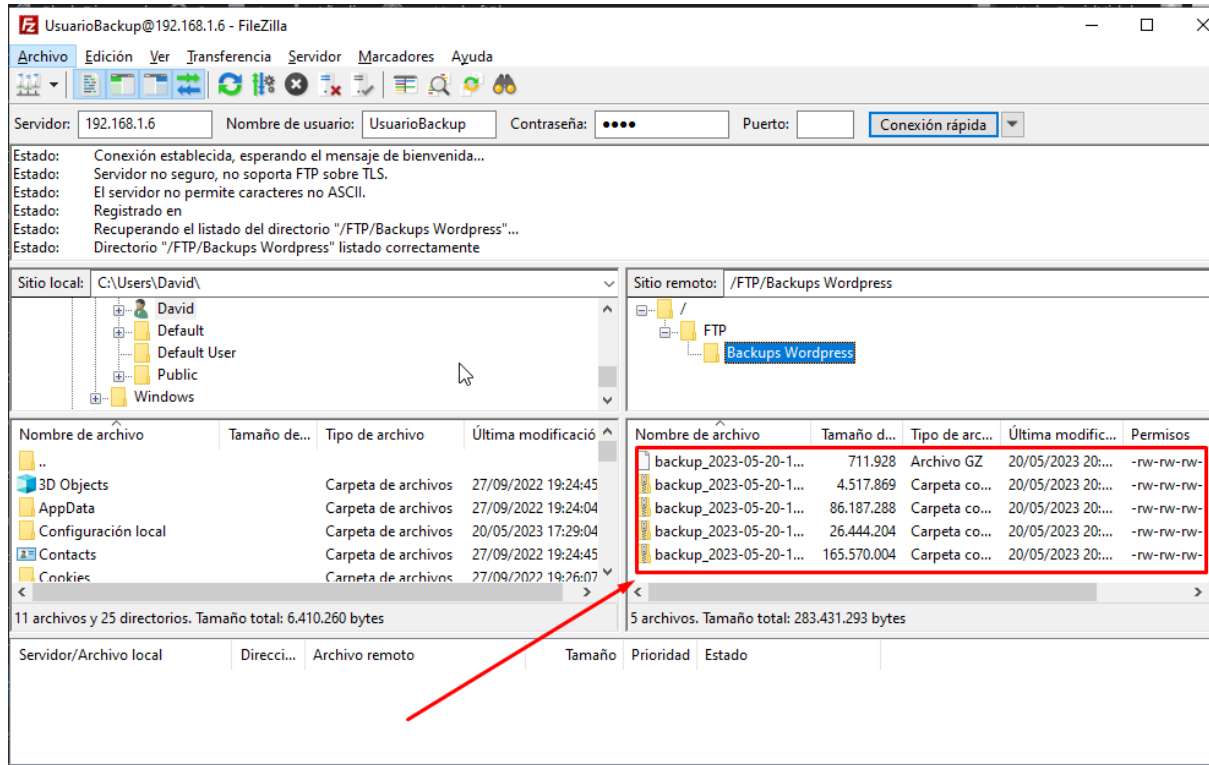
Seleccionaremos que queremos incluir en la copia de seguridad y también seleccionaremos que se envíe la copia de seguridad al almacenamiento remoto.



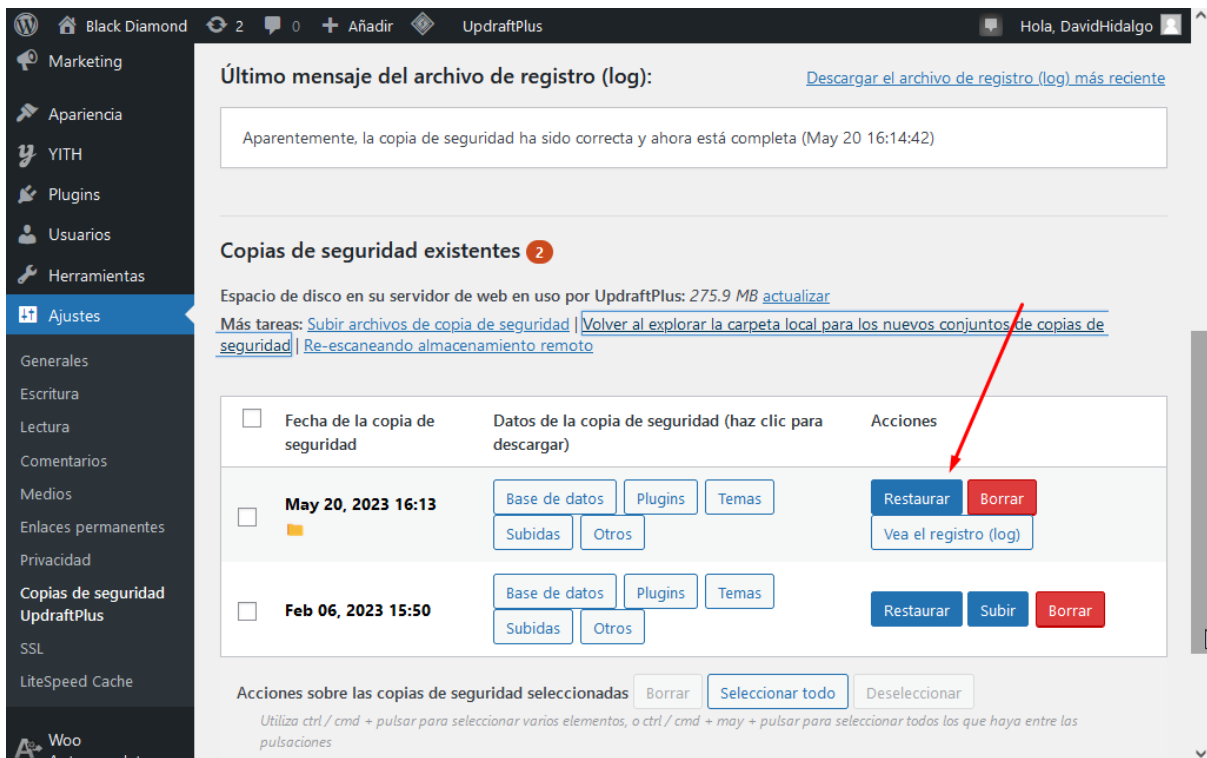
Comprobamos que se ha realizado correctamente.



Y ahora, si nos conectamos por FTP al servidor otra vez, podremos ver que tenemos las copias de seguridad en el servidor.



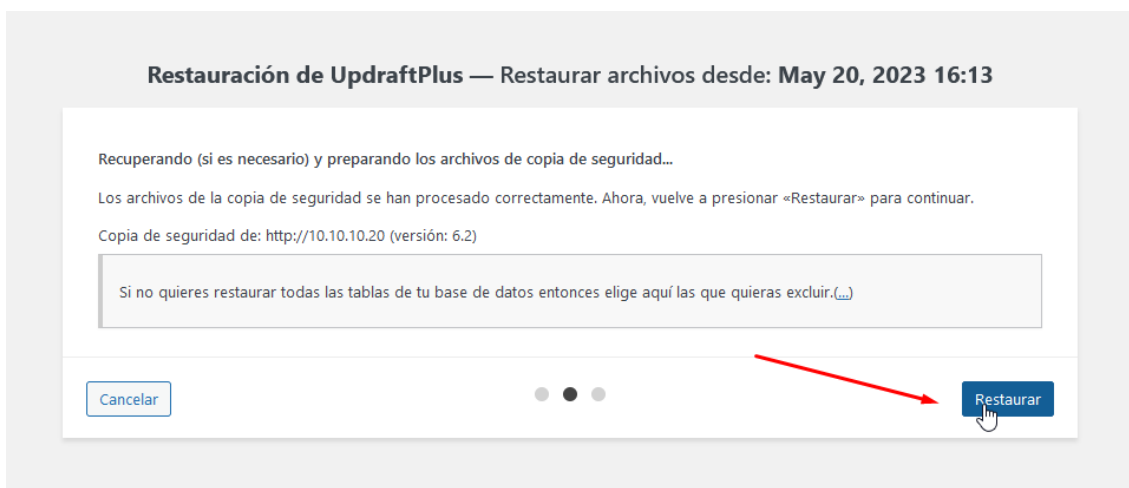
En caso de que queramos restaurar la web desde la copia de seguridad, entramos en el apartado del plug-in y en la zona de copias de seguridad existentes, le daremos a restaurar.



Seleccionamos los componentes a restaurar.



Le damos a Restaurar.



Esperamos un rato y ya tendremos la web restaurada.

Restauración de UpdraftPlus - Copia de seguridad May 20, 2023 16:13

La operación de restauración se ha iniciado (23ad25a6f181). No cierres esta página hasta que informe que ha finalizado.

Progreso de la restauración:

- ✓ Verificación
- ✓ Base de datos
- ✓ Plugins
- ✓ Temas
- ✓ Subidas
- ✓ Otros
- ✓ Limpieza
- ✓ Finalizado

Volver a la configuración de UpdraftPlus

[Sigue este enlace para descargar el archivo de](#)

Registro de actividad

```

Quitando de en medio los datos antiguos...
Moviendo la copia de seguridad desempaquetada a su lugar...
Limpiando basura...

Subidas
Descomprimiendo la copia de seguridad...
(backup_2023-05-20-1613_Black_Diamond_c813922c4888-uploads.zip,
157.9 MB)
Progreso de descompresión: 638 de 1139 archivos (100.2 MB,
uploads/2023/01/pexels-cottonbro-studio-3894389.jpg)
Progreso de descompresión: 1139 de 1139 archivos (160.6 MB,
uploads/woocommerce-placeholder-400x516.png)
Quitando de en medio los datos antiguos...
Moviendo la copia de seguridad desempaquetada a su lugar...
Limpiando basura...

Otros
Descomprimiendo la copia de seguridad...
(backup_2023-05-20-1613_Black_Diamond_c813922c4888-others.zip,
4.3 MB)
Progreso de descompresión: 455 de 455 archivos (15.4 MB, et-
cache/image_responsive_metadata.data)
Limpiando basura...
                    
```

Ahora continuaremos con la copia de seguridad de los usuarios de LDAP. Para eso, primero crearemos otra carpeta compartida en el servidor NAS.

The screenshot shows the 'Almacenamiento' section of the NAS interface. The 'Carpeta Compartidas' menu item is highlighted in the left sidebar. The main area displays a table of existing shares:

Nombre	Dispositivo	Ruta relativ	Ruta absoluta	Referenciad	Comentario
BD	/dev/md0	BD/	/srv/dev-disk-by-uuid-5b1f8363-d9f3-4add-aaa7-5b4e063f9065/BD	✓	
FTP	/dev/md0	FTP/	/srv/dev-disk-by-uuid-5b1f8363-d9f3-4add-aaa7-5b4e063f9065/FTP	✓	
UsuariosLD	/dev/md0	Usuarios	/srv/dev-disk-by-		

La llamaremos Usuarios LDAP.

openmediavault

NAS-proyecto6.blackdiamond.cat

Almacenamiento | Carpetas Compartidas | Crear

Nombre *
UsuariosLDAP

Sistema de Archivos *
/dev/md0 [Has sobrepasado el almacenamiento limite]

El sistema de archivos en el que será creada la carpeta compartida.
ruta relativa *
Usuarios LDAP/

La ruta relativa de la carpeta para compartir. La carpeta especificada se creará si no existe.
Permisos *
Administrador: Lectura/Escritura, Usuarios:Lectura/Escritura, Otros: Solo lectura

Modo de archivo de la ruta a las carpetas compartidas.
Comentario

Cancelar Salvar

Activar Windows
Ve a Configuración para activar Windows.

Seguidamente, iremos a Servicios>SMB/CIFS>Compartidos para crear una nueva carpeta compartida a través del Samba.

Dashboard

Sistema

Red

Almacenamiento

Servicios

FTP

NFS

Rsync

SMB/CIFS

Configuración

Compartidos

SSH SSH

NAS-proyecto6.blackdiamond.cat

Servicios | SMB/CIFS | Compartidos

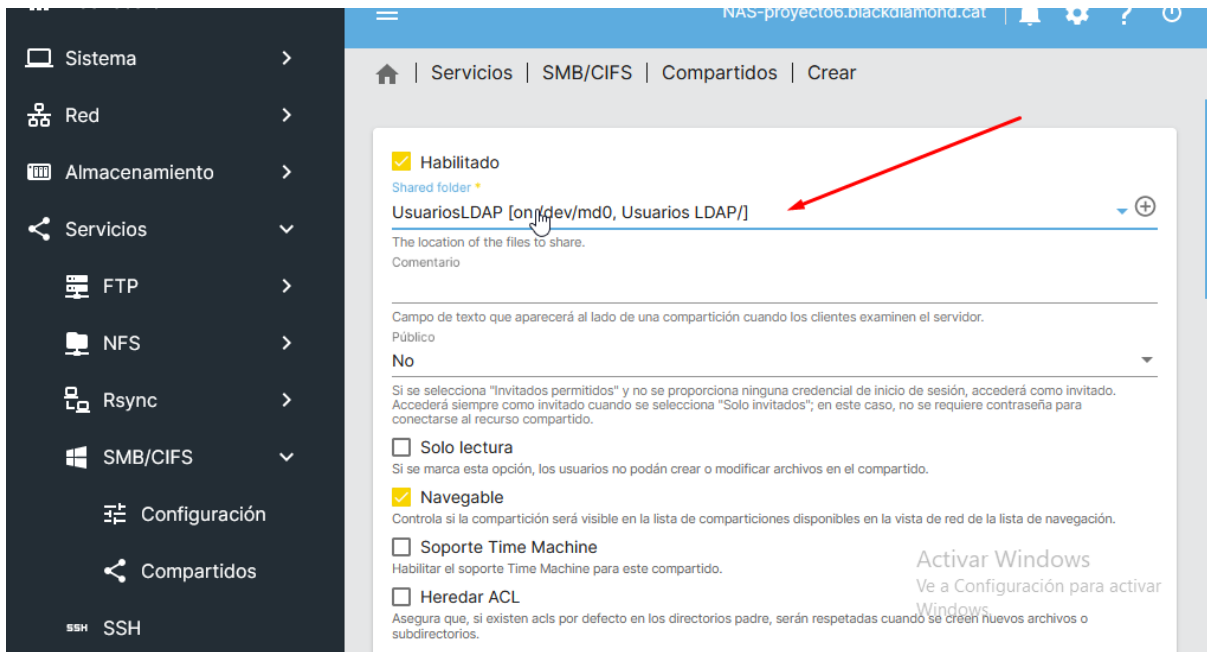
Crear

Compartido	Carpeta Comp	Comentario	Público	Solo lectura	Navegable
✓	BD			Guests allow	✓

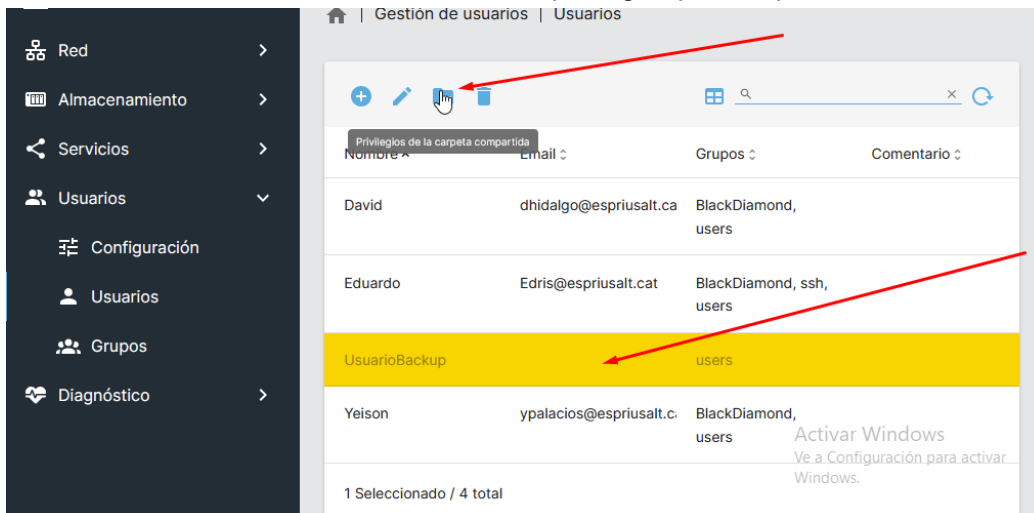
0 Seleccionado / 1 total

Activar Windows
Ve a Configuración para activar Windows.

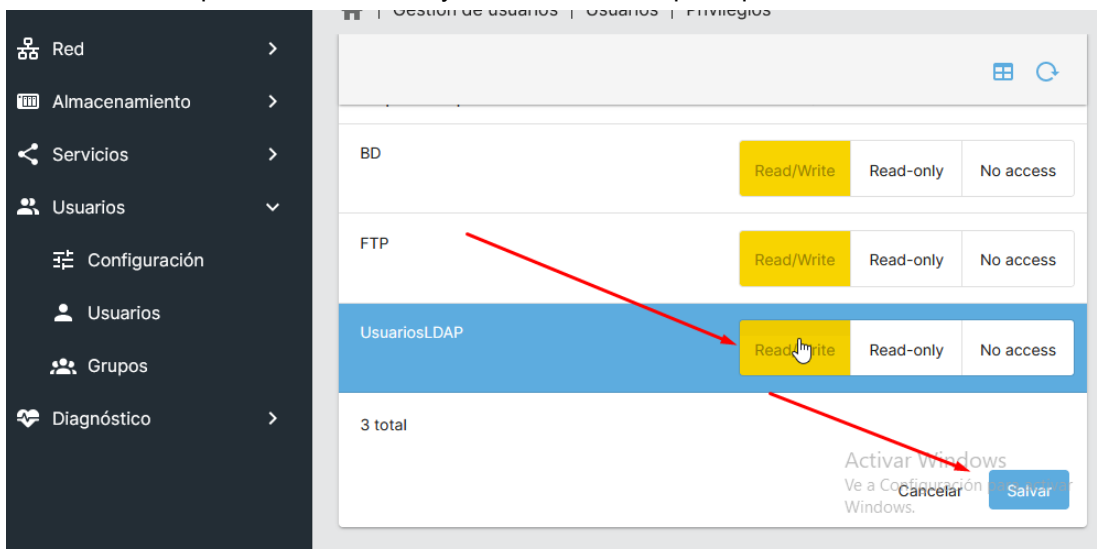
Seleccionaremos la carpeta que hemos creado de "Usuarios LDAP" y crearemos la carpeta compartida.



Dentro de usuarios, volveremos a cambiar los privilegios para carpetas del "UsuarioBackup"



Estableceremos permisos de lectura y escritura en la carpeta que acabamos de crear.



Ahora, dentro del terminal del servidor NAS, crearemos el directorio /etc/backup.


```
admin-dh@servidorLDAP:~$ sudo mkdir /etc/backup
```

Modificaremos los permisos de la carpeta a 700.

```
admin-dh@servidorLDAP:~$ sudo chmod -R 700 /etc/backup/
```

Y dentro del archivo fstab, añadiremos la carpeta compartida del NAS y la uniremos a la carpeta /etc/backup que hemos creado.

```
GNU nano 4.8 /etc/fstab
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/ubuntuvg/ubuntuvl during curtin installation
/dev/disk/by-id/dm-uuid-LVM-LSqKq9h2QXdUKmCpkKehux8v14USwp01FUPC3MvXyoe3uccLfqgZkaEJNx3Xc3q / ext4 defaults 0 1
# /boot was on /dev/sda2 during curtin installation
/dev/disk/by-uuid/56c24369-32fb-443f-80c6-658abb022a57 /boot ext4 defaults 0 1
/swap.img none swap sw 0 0
//192.168.1.6/UsuariosLDAP /etc/backup cifs username=UsuarioBackup,password=1234,uid=1000,gid=1000 0 0
```

Montaremos la carpeta compartida con el comando mount -a

```
admin-dh@servidorLDAP:~$ sudo mount -a
```

Ahora, crearemos un script llamado "ldap_backup.sh"

```
admin-dh@servidorLDAP:~$ nano ldap_backup.sh
```

Dentro añadiremos el siguiente contenido, el script guardará los datos del LDAP en la carpeta /etc/backup con la variante \$DATE, el cual será la fecha en la que se haga el backup.

```
GNU nano 4.8 ldap_backup.sh
#!/bin/bash
DATE=$(date +"%Y%m%d")

LDAP_SERVER="ldap://192.168.1.4"
LDAP_BASE_DN="dc=blackdiamond,dc=cat"
LDAP_USERNAME="cn=admin,dc=blackdiamond,dc=cat"
LDAP_PASSWORD="1234"

# Archivo de respaldo
BACKUP_FILE="${DATE}_backup.ldif"

# Realizar la copia de seguridad
ldapsearch -x -H "$LDAP_SERVER" -D "$LDAP_USERNAME" -w "$LDAP_PASSWORD" -b "$LDAP_BASE_DN" > "$BACKUP_FILE"
```

Y añadiremos el permiso de ejecución a este script.

```
admin-dh@servidorLDAP:~$ sudo chmod +x ldap_backup.sh
```

Ahora, haremos la automatización del script que acabamos de crear gracias a la herramienta crontab, utilizaremos el comando "crontab -e" para hacer una nueva tarea.

```
admin-dh@servidorLDAP:~$ crontab -e
no crontab for admin-dh - using an empty one

Select an editor. To change later, run 'select-editor'.
 1. /bin/nano        <---- easiest
 2. /usr/bin/vim.basic
 3. /usr/bin/vim.tiny
 4. /bin/ed

Choose 1-4 [1]: 1
crontab: installing new crontab
```

Dentro del archivo que se nos abrirá, escribimos lo siguiente, que hará que una vez al mes el sistema de archivo que deseamos y le daremos a salvar.

```

GNU nano 4.8 /tmp/crontab.yTxXLu/crontab
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
0 0 1 * * ./ldap_backup.sh

```

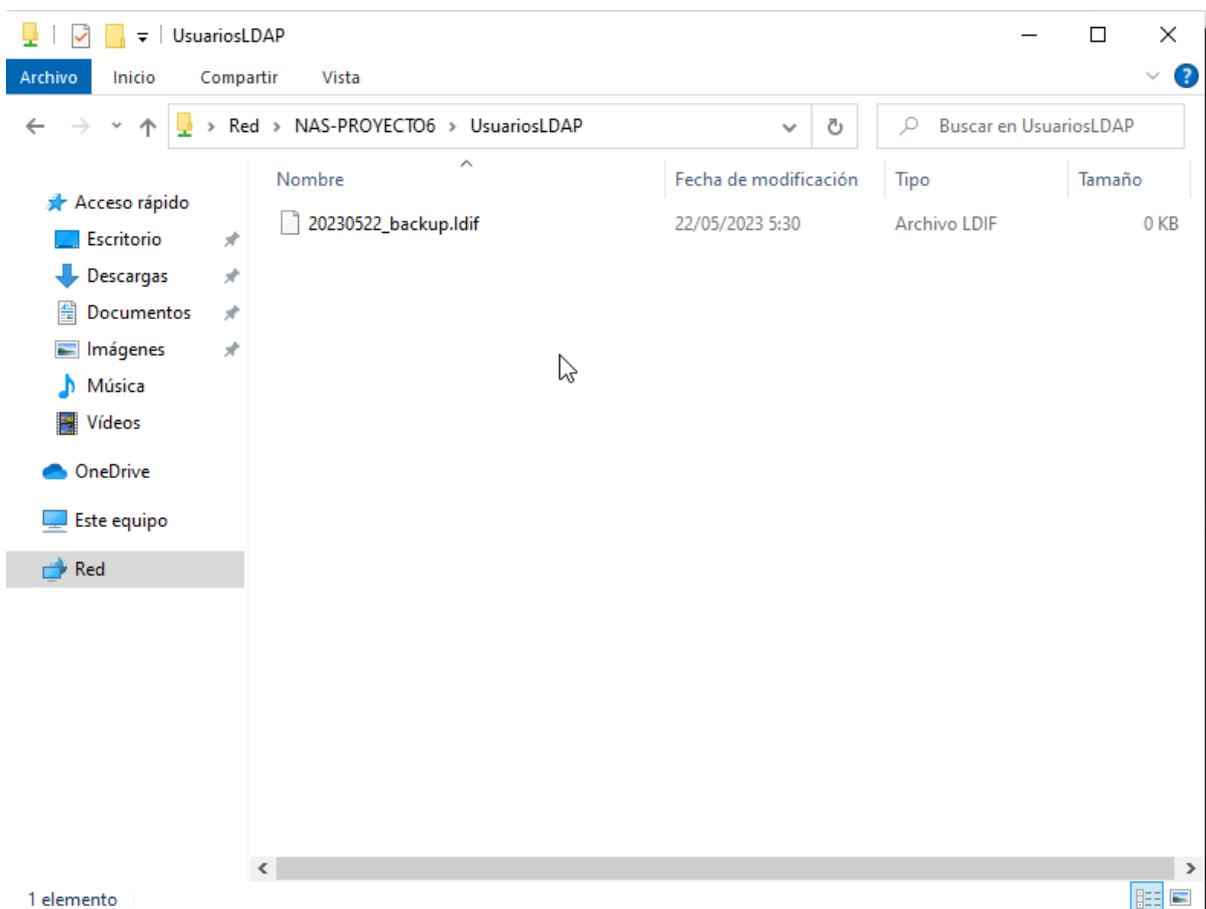
Para no tener que esperar un mes hasta que se ejecute el script, lo haremos nosotros manualmente.

```
ldap@servidorldap:~$ ./ldap_backup.sh
```

Si utilizamos el comando ls dentro de la carpeta de /etc/backup, podremos ver que tenemos la copia de seguridad hecha, con la fecha en la que se ha hecho.

```
ldap@servidorldap:~$ ls /etc/backup/
20230522_backup.ldif
```

También, comprobamos que el archivo de la carpeta está realmente compartido con el samba. Entrando desde un cliente al explorador de archivos y accediendo a la carpeta, podemos ver que el archivo .ldif, está creado.



2- Estableix criteris de complexitat de contrasenyes i contraatacs de força bruta per l'accés als equips.

Ante todo, tendremos que entrar en la carpeta siguiente:

```
ldap@servidorldap:~$ cd /etc/ldap/slapd.d/
```

Con este comando, activaremos el overlay del módulo "ppolicy"

```
ldap@servidorldap:/etc/ldap/slapd.d$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/ppolicy.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=ppolicy,cn=schema,cn=config"
```

Crearemos un archivo .ldif con el siguiente contenido:

```
ldap@servidorldap:/etc/ldap/slapd.d$ cat myouppolicy.ldif
dn: ou=Policies,dc=blackdiamond,dc=cat
objectClass: top
objectClass: organizationalUnit
ou: Policies
description: My Organization policies come here
```

Con este comando, crearemos la unidad organizativa "Policies", donde meteremos las políticas para las contraseñas.

```
ldap@servidorldap:/etc/ldap/slapd.d$ sudo ldapadd -D cn=admin,dc=blackdiamond,dc=cat -w 1234 -f myouppolicy.ldif
adding new entry "ou=Policies,dc=blackdiamond,dc=cat"
```

Crearemos otro archivo .ldif con el siguiente contenido:

```
ldap@servidorldap:/etc/ldap/slapd.d$ cat pppolicy.ldif
dn: cn=module{0},cn=config
changetype: modify
add: olcModuleLoad
olcModuleLoad: pppolicy
```

Cargaremos el archivo que acabamos de crear, para cargar el módulo pppolicy

```
ldap@servidorldap:/etc/ldap/slapd.d$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f pppolicy.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "cn=module{0},cn=config"
```

Crearemos un archivo .ldif con el siguiente contenido:

```
ldap@servidorldap:/etc/ldap/slapd.d$ cat pppolicyoverlay.ldif
dn: olcOverlay={0}ppolicy,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcPPolicyConfig
olcOverlay: {0}ppolicy
olcPPolicyDefault: cn=MyOrgPPolicy,ou=Policies,dc=blackdiamond,dc=cat
```

Cargaremos el archivo que acabamos de crear, para así preparar el overlay de pppolicy.

```
ldap@servidorldap:/etc/ldap/slapd.d$ sudo ldapadd -Y EXTERNAL -H ldapi:/// -f pppolicyoverlay.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "olcOverlay={0}ppolicy,olcDatabase={1}mdb,cn=config"
```

Crearemos un archivo .ldif con los parámetros que nosotros queramos establecer para las contraseñas. Los parámetros más importantes son los siguientes:

- **pwdMinLength**: La longitud mínima de la contraseña es de 8 caracteres.
- **pwdMaxAge**: La contraseña caduca después de 30 días (2592000 segundos).
- **pwdInHistory**: Las últimas 5 contraseñas utilizadas no se pueden volver a utilizar.

- `pwdCheckQuality`: Se verifica la calidad de la contraseña (2 para una verificación básica).
- `pwdMaxFailure`: Se permite un máximo de 3 intentos de inicio de sesión fallidos.
- `pwdLockout`: Se bloquea la cuenta después de exceder el número máximo de intentos fallidos.
- `pwdLockoutDuration`: La cuenta se bloquea durante 1800 segundos (30 minutos).
- `pwdGraceAuthNLimit`: No se permite el acceso después de la cuenta bloqueada.
- `pwdFailureCountInterval`: El recuento de intentos de inicio de sesión fallidos se restablece inmediatamente.
- `pwdMustChange`: Se requiere un cambio de contraseña al inicio de sesión.

```

ldap@servidorldap:/etc/ldap/slapd.d$ cat passwordpolicy.ldif
dn: cn=default,ou=Policias,dc=blackdiamond,dc=cat
changetype: add
objectClass: top
objectClass: device
objectClass: pwdPolicy
cn: default
pwdAttribute: userPassword
pwdMaxAge: 2592000
pwdExpireWarning: 604800
pwdInHistory: 5
pwdCheckQuality: 2
pwdMinLength: 8
pwdMaxFailure: 3
pwdLockout: TRUE
pwdLockoutDuration: 1800
pwdGraceAuthNLimit: 0
pwdFailureCountInterval: 0
pwdMustChange: TRUE

dn: cn=passwordPolicyEntry,ou=Policias,dc=blackdiamond,dc=cat
changetype: modify
replace: pwdMinLength
pwdMinLength: 8
-
replace: pwdMaxAge
pwdMaxAge: 2592000
-
replace: pwdInHistory
pwdInHistory: 5
-
replace: pwdCheckQuality
pwdCheckQuality: 2

```

Cargaremos el archivo que acabamos de crear, para aplicar los parámetros definidos anteriormente.

```

ldap@servidorldap:/etc/ldap/slapd.d$ sudo ldapadd -D cn=admin,dc=blackdiamond,dc=cat -w 1234 -f passwordpolicy.ldif
adding new entry "cn=default,ou=Policias,dc=blackdiamond,dc=cat"

```

Ahora, crearemos un archivo .ldif para la creación de un usuario "test" y comprobar el funcionamiento.

```
ldap@servidorldap:/etc/ldap/slapd.d$ cat users.ldif
dn: ou=Users,dc=blackdiamond,dc=cat
description: My Organization Users come here
objectclass: top
objectclass: organizationalUnit
ou: Users

dn: uid=test,ou=Users,dc=blackdiamond,dc=cat
cn: test
sn: test
uid: test
ou: Users
objectClass: organizationalPerson
objectClass: inetOrgPerson
```

Añadimos el archivo .ldif para crear el usuario dentro del LDAP.

```
ldap@servidorldap:/etc/ldap/slapd.d$ sudo ldapadd -D cn=admin,dc=blackdiamond,dc=cat -w 1234 -f users.ldif
adding new entry "ou=Users,dc=blackdiamond,dc=cat"

adding new entry "uid=test,ou=Users,dc=blackdiamond,dc=cat"
```

Y le generamos una contraseña al usuario que acabamos de crear. Como podemos ver, es de 8 caracteres y tiene mayúsculas y minúsculas.

```
ldap@servidorldap:/etc/ldap/slapd.d$ sudo ldappasswd -D cn=admin,dc=blackdiamond,dc=cat -w 1234 'uid=test,ou=users,dc=blackdiamond,dc=cat'
New password: 4trDN.rP
```

Con el siguiente comando, podemos ver que se han hecho los cambios en la configuración de la base de LDAP.

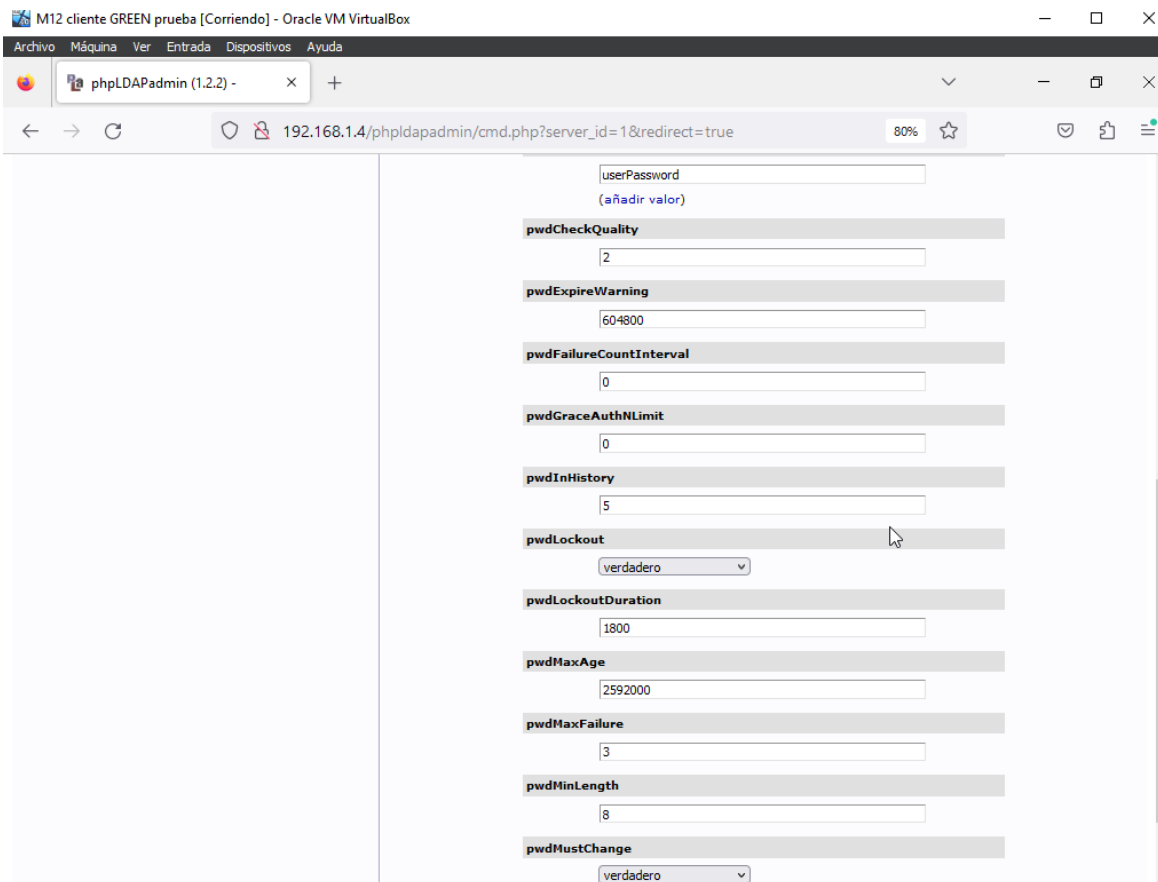
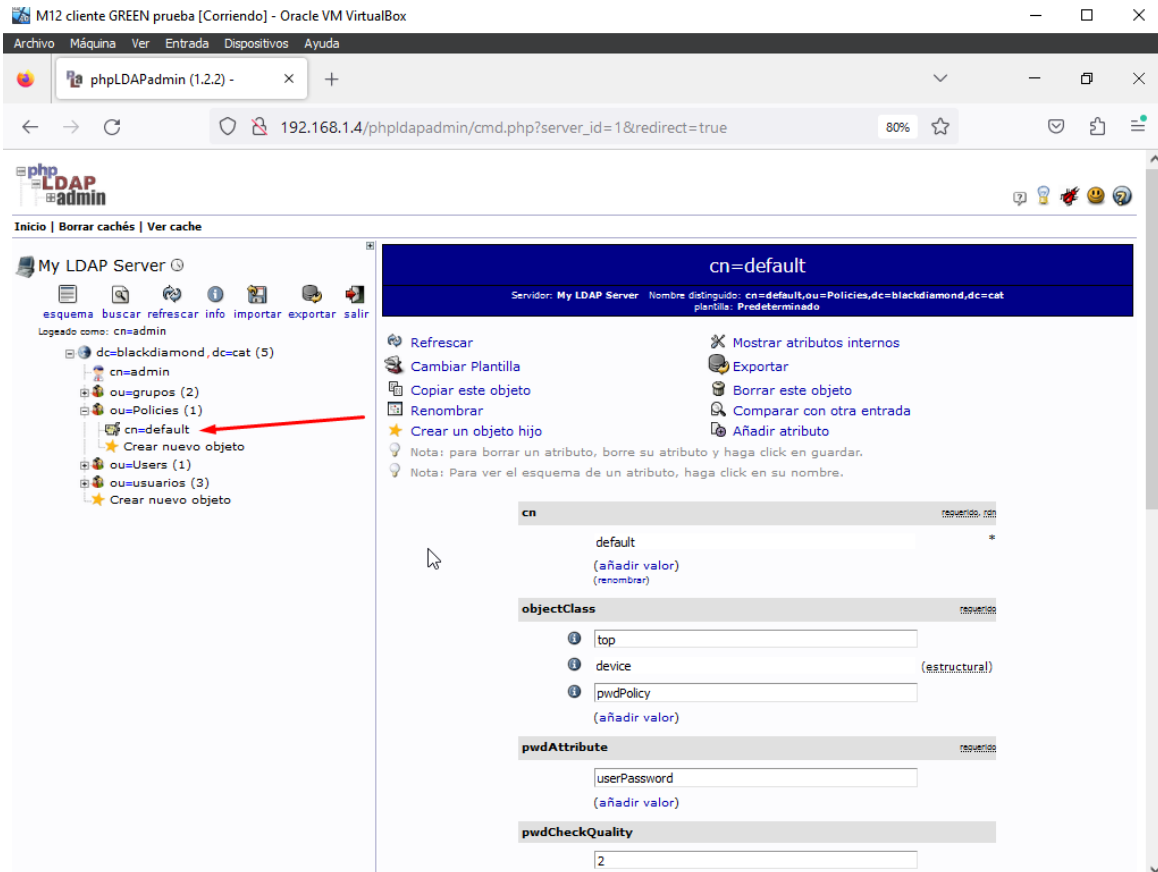
```
ldap@servidorldap:/etc/ldap/slapd.d$ sudo ldapsearch -Y EXTERNAL -H ldapi:/// -b olcDatabase={1}mdb,cn=config
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
# extended LDIF
#
# LDAPv3
# base <olcDatabase={1}mdb,cn=config> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# {1}mdb, config
dn: olcDatabase={1}mdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcMdbConfig
olcDatabase: {1}mdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=blackdiamond,dc=cat
olcAccess: {0}to attrs=userPassword by self write by anonymous auth by * none
olcAccess: {1}to attrs=shadowLastChange by self write by * read
olcAccess: {2}to * by * read
olcLastMod: TRUE
olcRootDN: cn=admin,dc=blackdiamond,dc=cat
olcRootPW: {SSHA}DLhBs7KFhdzK0WY79+a4kTSxexV/WCPi
olcDbCheckpoint: 512 30
olcDbIndex: objectClass eq
olcDbIndex: cn,uid eq
olcDbIndex: uidNumber,gidNumber eq
olcDbIndex: member,memberUid eq
olcDbMaxSize: 1073741824

# {0}ppolicy, {1}mdb, config
dn: olcOverlay={0}ppolicy,olcDatabase={1}mdb,cn=config
objectClass: olcOverlayConfig
objectClass: olcPPolicyConfig
olcOverlay: {0}ppolicy
olcPPolicyDefault: cn=MyOrgPPolicy,ou=Policies,dc=blackdiamond,dc=cat

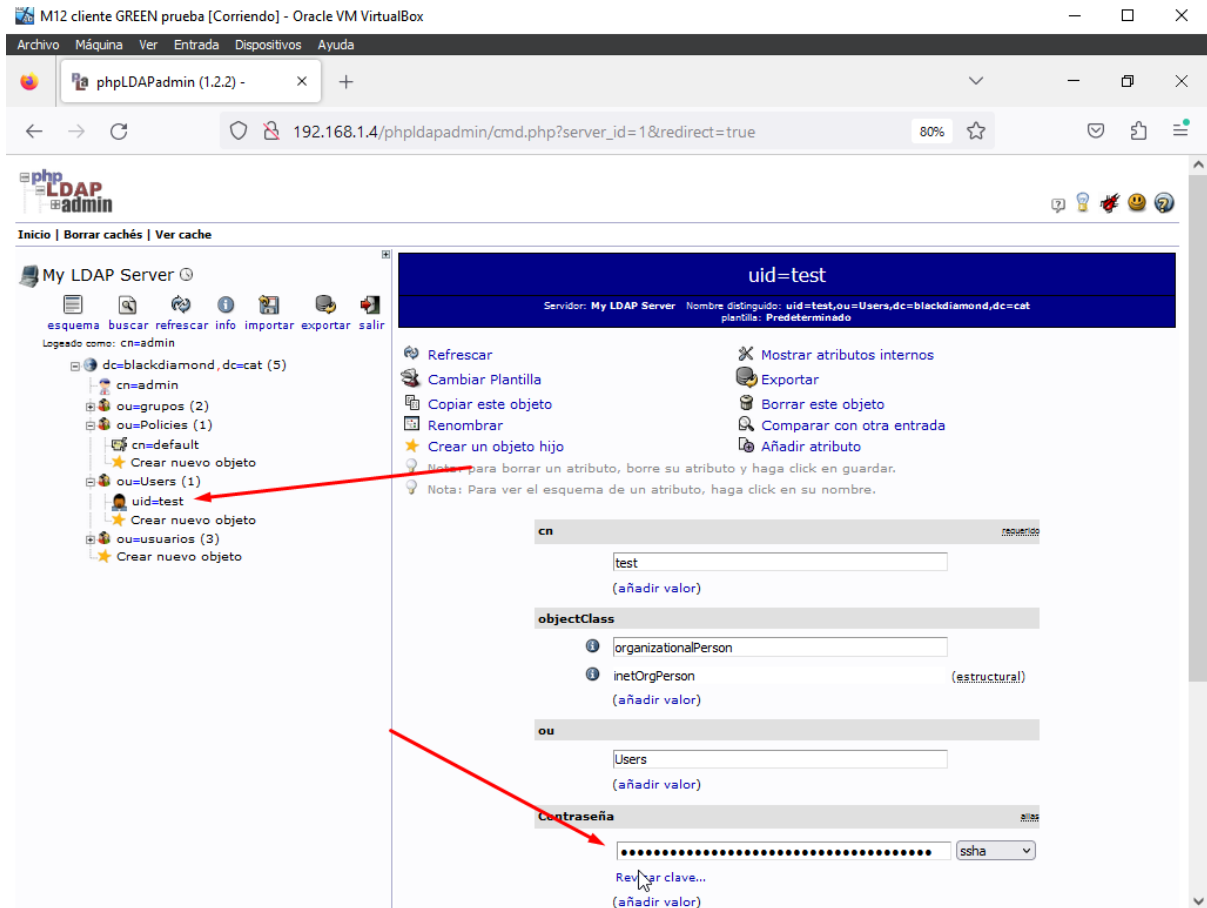
# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
ldap@servidorldap:/etc/ldap/slapd.d$
```

Si entramos en el **phpLDAPadmin**, podremos ver que se ha creado la política de las contraseñas.



Y también se ha creado el usuario test con la contraseña.



Conclusión

En este proyecto se han aplicado bastantes cosas a las que se les podría dar una gran utilidad en caso de encontrarse trabajando en una empresa o estar creando una empresa propia. Consideramos que la utilización de un firewall con DMZ y un proxy puede ser algo muy útil a la hora de tener una red privada con ciertas restricciones y seguridad. En caso de la instalación del NAS con sus copias de seguridad automáticas hemos aprendido a instalar y configurar un NAS haciendo sus respectivos RAID y carpetas compartidas para una empresa, el poder utilizar un sistema de almacenamiento en red también puede ser muy cómodo para que diversos usuarios tengan acceso a la información sin la necesidad de ocupar espacio en cada uno de los equipos en los que esta información sea necesaria.

En conclusión creemos que ha sido un buen proyecto y bastante útil a excepción de los problemas que han habido durante el transcurso de dicho proyecto (Durante dos días y medio de proyecto no ha habido acceso a internet en la red INFOESPRIU por lo que no se ha podido avanzar demasiado debido a que la red GENCAT es una red con una conexión a internet muy lenta y demasiadas restricciones.)